IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

INTELLECTUAL VENTURES I LLC, and INTELLECTUAL VENTURES II LLC, Plaintiffs, v. HEWLETT PACKARD ENTERPRISE COMPANY, Defendant.	Civil Action No. ______________ **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs, Intellectual Ventures I LLC ("Intellectual Ventures I") and Intellectual Ventures II LLC ("Intellectual Ventures II") (collectively "IV" or "plaintiffs") for their complaint against defendant, Hewlett Packard Enterprise Company ("HPE"), allege as follows:

THE PARTIES

1. Intellectual Ventures I is a Delaware limited liability company having its principal place of business located at 3150 139th Avenue SE, Bellevue, Washington 98005.

2. Intellectual Ventures II is a Delaware limited liability company having its principal place of business located at 3150 139th Avenue SE, Bellevue, Washington 98005.

3. HPE is a corporation organized under the laws of Delaware.

JURISDICTION

4. Plaintiffs bring this action for patent infringement pursuant to 35 U.S.C. § 281, *et seq.* This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

FACTUAL BACKGROUND

5. Intellectual Ventures Management, LLC ("Intellectual Ventures") was founded in 2000. Intellectual Ventures fosters inventions and facilitates the filing of patent applications for those inventions; collaborates with others to develop and patent inventions; and acquires and licenses patents from individual inventors, universities, corporations, and other institutions. A significant aspect of Intellectual Ventures's business is managing the plaintiffs in this case.

6. One founder of Intellectual Ventures is Nathan Myhrvold, who worked at Microsoft from 1986 until 2000 in a variety of executive positions, culminating in his appointment as the company's first Chief Technology Officer in 1996. While at Microsoft, Dr. Myhrvold founded Microsoft Research in 1991 and was one of the world's foremost software experts. Between 1986 and 2000, Microsoft became the world's largest technology company.

7. Under Dr. Myhrvold's leadership, Intellectual Ventures acquired thousands of patents covering many important inventions of the Internet era, including many pertaining to the networked computers that comprise the Internet. Many of these inventions coincided with or shortly followed Dr. Myhrvold's successful tenure at Microsoft.

8. HPE makes, uses, and sells 802.11 Wi-Fi access points ("APs") in the United States including the Aruba line of APs. This line includes the Aruba 303 Series Indoor Wi-Fi 5 Access Point, the Aruba 500 Series Indoor Access Point, and the Aruba 510 Series Indoor Access Point. According to HPE, these APs comprise technologies including ClientMatch and ARM ("Adaptive Radio Management"). ClientMatch "continuously monitors the health of all clients connected to each access point, intelligently grouping them," while "ARM automatically assigns channel, width, and power settings based on environment and client density." See

https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/303-series/.

9. In addition, HPE makes, uses, and sells 802.11ax-based (Wi-Fi 6) APs, including AP-505, AP-515, AP-534, AP-535, and AP-555, that implement ArubaOS 8.6.0.0 and later, and that support the Basic Service Set ("BSS") coloring mechanism with simultaneous transmissions of overlapping BSSs. See https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/whats_new.htm.

10. In addition, HPE makes, uses, and sells 802.11n-based, 802.11ac-based, and 802.11ax-based APs, including at least the Aruba 600 Series of APs, and the Aruba 650 Series Wi-Fi 6E Campus Access Point line of products. See https://www.exclusive-networks.com/nl/wp-content/uploads/sites/21/2022/02/ DS_AP650Series.pdf.

THE PATENTS-IN-SUIT

11. On March 1, 2022, the United States Patent and Trademark Office ("USPTO") issued United States Patent No. 11,265,787 ("the '787 patent"), titled PROGRAM FOR ADJUSTING CHANNEL INTERFERENCE BETWEEN ACCESS POINTS IN A WIRELESS NETWORK, attached as Exhibit A. The '787 patent is valid and enforceable.

12. Intellectual Ventures II is the owner and assignee of all rights, title, and interest in the '787 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

13. The '787 patent is directed to improved systems and methods of wireless communication, including the provision of more seamless roaming for Wi-Fi wireless stations ("STAs"). According to embodiments, Wi-Fi APs coordinate with each other and with other

components of Wi-Fi networks (e.g., wireless local area networks, or WLANs) by exchanging frames indicating whether frequency channels are available or unavailable, to perform automatic channel selection, power management, and load balancing. The performance and ease of management of Wi-Fi networks is improved by the technologies disclosed and claimed in the ’787 patent such that channel usage and seamless roaming are optimized, while minimizing interference.

14. On January 14, 2014, the USPTO reissued United States Patent No. 7,773,944 as US RE44,439 (“the ’706 patent”), titled RF DOMAINS, attached as Exhibit B. The ’706 patent is valid and enforceable.

15. Intellectual Ventures II is the owner and assignee of all rights, title, and interest in the ’706 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

16. The ’706 patent is also directed to improved systems and methods of wireless communication. According to embodiments, a wireless device such as an AP may broadcast a unique identifier for a service set supported by that wireless device. The wireless device also listens to wireless messages broadcast by other wireless devices, e.g., other APs, for such identifiers. If the wireless device discovers another wireless device, e.g., another AP, that supports a same service set on the same frequency channel (i.e., an overlapping service set), the wireless device may reduce its transmission power so as not to interfere with transmissions emitted by the other wireless device that are associated with the overlapping service set. The transmit power of communications associated with non-overlapping service sets is not affected by the patented transmit power reduction method and apparatus. The performance of wireless networks is thereby improved by the technologies disclosed and claimed in the ’706 patent.

17. On November 24, 2009, the USPTO issued United States Patent No. 7,623,439 ("the '439 patent"), titled CYCLIC DIVERSITY SYSTEMS AND METHODS, attached as Exhibit C. The '439 patent is valid and enforceable.

18. Intellectual Ventures I is the owner and assignee of all rights, title, and interest in the '439 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

19. The '439 patent is also directed to improved systems and methods of wireless communication. One exemplary embodiment comprises an improved cyclic diversity system in which a logic circuit is configured to cyclically advance samples of a symbol data portion of an orthogonal frequency division multiplexing (OFDM) packet to be transmitted on a first antenna, relative to the samples of a symbol data portion of another OFDM packet to be transmitted on another antenna. The duration of the cyclic advance is less than the duration of a guard interval portion of the OFDM packet. By using a cyclic advance as described above, the symbol data portions of the two different transmitted signals are better decorrelated, thus reducing the probability of unintentional beamforming. The performance of wireless networks is thereby improved by the technologies disclosed and claimed in the '439 patent.

COUNT I

(HPE's Infringement of U.S. Patent No. 11,265,787)

20. The preceding paragraphs are incorporated by reference.

21. The '787 patent claims and teaches improved APs capable of collectively working together and with other components of a Wi-Fi network to perform automatic channel selection, power management, and load balancing, while avoiding mutual interference. They do so by receiving channel selection and power level information from other components of the wireless

network. This information is used to perform automatic channel selection and power management, even as radio conditions change and as STAs roam between APs. An AP is able to store the information resulting from such operations indicating which, if any, channels are available and which, if any, channels are unavailable. Each AP is thereby enabled to communicate on certain available channels and at certain power levels that are set based on information received from other components of the wireless network to improve overall system performance.

22. Prior art systems associated a given STA with a given AP on a given frequency channel, without using certain information available at other APs or STAs that could be used to optimize those associations. The claims of the ’787 patent recite a wireless communication capable device comprising a transceiver and a processor where the transceiver and the processor are configured to receive a wireless signal that includes a medium access control (MAC) message that has that information. Specifically, the MAC message includes information multiplexed with other data. The information may comprise an indication that a frequency channel is unavailable or that a frequency channel is available. In response to information indicating that a frequency channel from a set of frequency channels is unavailable, the processor is configured to store information indicating that the frequency channel is unavailable. Similarly, in response to information indicating that a frequency channel from a set of frequency channels is available, the processor is configured to store information indicating that the frequency channel is available. This process enables the transceiver and the processor to be configured to effectively communicate in the dynamic radio frequency (“RF”) environment of most Wi-Fi networks using available frequency channels from the set of frequency channels.

23. This communication allows an AP to physically store information based in part on the contents of the MAC messages, relating one or more frequencies within a set of frequencies as being available or unavailable. This communication allows the AP to physically store information based in part on the contents of the MAC messages relating one or more frequencies within a set of frequencies as being available or unavailable. Such storage in turn enables the AP to subsequently communicate more effectively in the dynamic RF environment of most Wi-Fi networks.

24. HPE has directly infringed and continues to directly infringe at least claim 4 of the ’787 patent by making, using, selling, offering for sale, and importing products and services covered by that patent’s claims. HPE’s products and services that infringe the ’787 patent include the line of Aruba 303 Series Indoor Wi-Fi 5 Access Points (including Instant OS) incorporating “ClientMatch” and “Adaptive Radio Management” (“ARM”) technologies; the line of Aruba 500 Series Access Points (including Instant OS) incorporating “ClientMatch” and ARM technologies; the line of Aruba 510 Series Indoor Access Points (including Instant OS) incorporating “ClientMatch” and ARM”; and all other Aruba access point products or components (including Instant OS) incorporating “ClientMatch” and “ARM” made, used, sold, or offered for sale by or on behalf of HPE (collectively, “the ’787 Accused Products”).

25. Claim 4 of the ’787 patent, written in independent form, is reproduced below:

4. [*A wireless communications capable device comprising:*

a transceiver; and

a processor;

wherein the transceiver and the processor are configured to receive a wireless signal, the wireless signal including a medium access control (MAC) message, wherein the MAC message includes information multiplexed with other data;

wherein, in response to the information indicating that a frequency channel is unavailable, the processor is configured to store information indicating that the frequency channel is unavailable from a set of frequency channels;

wherein, in response to the information indicating that the frequency channel is available, the processor is configured to store information indicating that the frequency channel is available from the set of frequency channels; and

wherein the transceiver and the processor are configured to communicate using available frequency channels from the set of frequency channels]

wherein the processor determines a power level based on a received signal strength of the wireless signal.

26. The ’787 Accused Products each provide a wireless communications capable device comprising a transceiver and a processor. As one example, the ’787 Accused Products comprise APs that are configured for wireless communication within a WLAN, as seen below with respect to the Aruba 303 Series Indoor Wi-Fi 5 Access Point:

Source: https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/303-series/

Model	Version	SoC	CPU MHz	Flash MB	RAM MB	WLAN Hardware	WLAN2.4	WLAN5.0
AP-303		Qualcomm IPQ4029	716	128NAND	512	Qualcomm Atheros IPQ4019	b/g/n	a/n/ac

Source: https://openwrt.org/toh/aruba/ap-303

SPECIFICATIONS

Hardware Variants

- AP-303 models: single Ethernet
- AP-303P models: second Ethernet with PoE out

Wi-Fi Radio Specifications

- AP type: Indoor, dual radio, 5GHz 802.11ac 2x2 MIMO and 2.4GHz 802.11n 2x2 MIMO
- 5GHz (radio 0):
  - Two spatial stream Single User (SU) MIMO for up to 867 Mbps wireless data rate to individual 2SS VHT80 client devices
  - Two spatial stream Multi User (MU) MIMO for up to 867 Mbps wireless data rate to two 1SS MU-MIMO capable client devices simultaneously
- 2.4GHz (radio 1):
  - Two spatial stream Single User (SU) MIMO for up to 300 Mbps wireless data rate to individual 2SS HT40 client devices

Source: https://www.arubanetworks.com/assets/ds/DS_AP303Series.pdf

27. The transceiver and the processor of the ’787 Accused Products are configured to receive a wireless signal. As an example, they are configured to receive wireless signals from client devices (i.e., STAs):

ARUBA 303 SERIES CAMPUS ACCESS POINTS

- AP type: Indoor, dual radio, 5GHz 802.11ac 2x2 MIMO and 2.4GHz 802.11n 2x2 MIMO

Source: https://www.arubanetworks.com/assets/ds/DS_AP303Series.pdf

The promise of 802.11n networks is to provide “wire like” speeds to the end user, eventually as much as 600 Mb/s per radio. This speed is achievable by using multiple technologies, including the use of multiple-input and multiple-output (MIMO) technology. MIMO technology combines multiple send and receive antennas, and multiple streams of data being sent at the same time. In addition, the 802.11n specification adds new encoding algorithms and wider channels. This all comes together to increase the data transfer rate significantly.

Transmit, Receive, and Spatial Streams

With 802.11a/b/g, only a single set of antennas and a single stream of data are involved. However, 802.11n adds multiple antennas and multiple streams of data to increase the transmission capabilities of APs and stations. As mentioned previously, it is important to check the transmit, receive, and spatial streams that are supported by the AP.

- Transmit: The number of antennas that are dedicated to transmitting data.
- Receive: The number of antennas that are dedicated to receiving data.
- Spatial streams: The number of individual data streams that the radio is capable of transmitting. An 802.11 a/b/g AP (1 x 1 : 1) is capable of one stream of data, or one transmission, to a client

Source: https://www.arubanetworks.com/vrd/80211nNetworksVRD/wwhelp/wwhimpl/js/html/wwhelp.htm

The Aruba AP-303 is a 2×2 802.11ac Wave 2 access point. It is fairly powerful with a quad-core ARM processor and 512 MB of memory. The Aruba Instant On AP11 is a much cheaper version of this device and is based on the same platform, the OpenWrt firmware for Aruba AP-303 can also be flashed onto the Aruba Instant On AP11.

Source: https://openwrt.org/toh/aruba/ap-303

Aruba 550 Series Indoor Access Points

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature supersedes the legacy band steering and spectrum load balancing features, which, unlike client match, do not trigger IAP changes for clients already associated to an IAP. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an IAP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- **Dynamic Load Balancing**: Client match balances clients across IAPs on different channels, based on the client load on the IAPs and the SNR levels the client detects from an underutilized IAP. If an IAP radio can support additional clients, the IAP will participate in client match load balancing and clients can be directed to that IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.
- **Sticky Clients**: The client match feature also helps mobile clients that tend to stay associated to an IAP despite low signal levels. IAPs using client match continually monitor the client's RSSI as it roams between IAPs, and move the client to an IAP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that IAP.
- **Band Steering**: IAPs using the client match feature monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 GHz radio, the IAP steers the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the IAP retains a suitable distribution of clients on each of its radios.

Source: https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

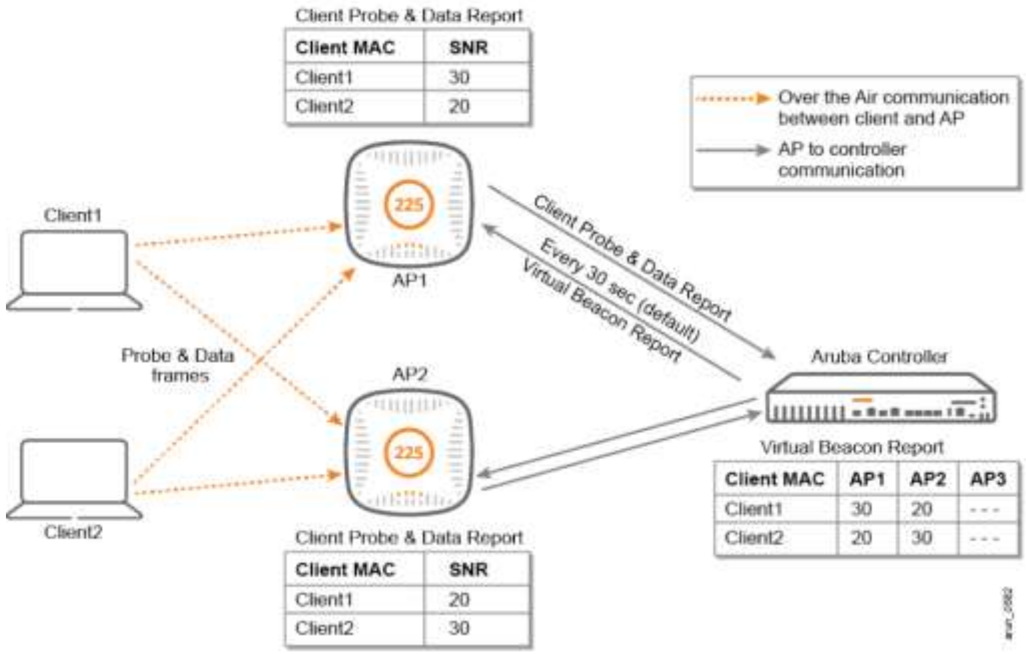
Aruba 550 Series Indoor Access Points

Selecting Optimal ClientMatch Settings

The ClientMatch figure shows how ClientMatch monitors each client's capabilities and connection on a WLAN using probe requests and data frames sent by the client.

- Each AP forms a client probe and data report, which includes a list of all the clients that an AP can hear, including the SNR.
- By default every 30 seconds APs send out this information to the controller, based on which a Virtual Beacon Report (VBR) is created, this maps each client to all the radios that can hear the client. Aruba controller sends out virtual beacon report of each client to the AP it is associated with.
- Based on the information received in the Virtual Beacon Report, an AP may decide to initiate band steering or sticky move for the clients associated to it. The decision to dynamically load balance the clients is however taken by the controller and not the APs.
- When a ClientMatch is initiated to move a client to the desired radio, all the radios in the RF vicinity except the one selected, blacklist the client for a short duration (default: 10 sec). This ensures that the client moves to the desired radio.

Figure 3 *ClientMatch Functionality*



To allow the Instant AP and clients to exchange neighbor reports, ensure that Client Match is enablec through **RF > ARM > Client match > Enabled** in the WebUI or by executing the **client-match** command in the **arm** configuration sub-command mode.

Source: https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

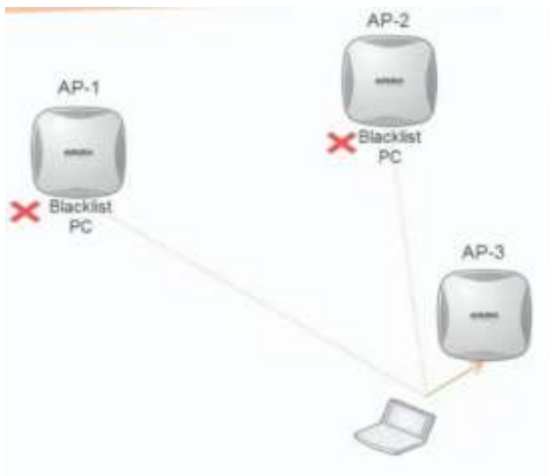
28. The wireless signal includes a MAC message that includes information multiplexed with other data. For example, if STAs and APs are 802.11k compliant, the STAs and APs can exchange MAC messages informing each other of other radios they each detect:

How ClientMatch Works

First, the clients associate to a radio. Next, all of the APs report probe requests from clients (as long as it's a good signal). If the client is 802.11k compliant, then the client informs the AP of other radios.

Then the controller builds a VBR (virtual beacon report) for ea ch client and shares this with the associated AP. The AP now has visibility into all available radios (APs) for this client. The AP now determines the optimum radio for this client.

Source: https://quizlet.com/433675597/ar-acma-8-dynamic-rf-management-flash-cards/



Source: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=22791

Radio Resource Management (802.11k)

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions.

4.3.11.11 Link measurement

The link measurement request/report exchange provides measurements of the RF characteristics of a STA-to-STA link. This measurement indicates the instantaneous quality of a link.

4.3.11.2 Beacon

The Beacon request/report pair enables a STA to request from another STA a list of APs whose beacons it can receive on a specified channel or channels. The Beacon report request/response provides a means for a requesting STA to obtain received beacon, probe response, and measurement pilot information from a responding STA.

6.3.32 Neighbor report request

6.3.32.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-NEIGHBORREPREQ.request(
                            DialogToken,
                            SSID,
                            LCI Measurement Request,
                            Location Civic Measurement Request,
                            VendorSpecificInfo
                            )
```

6.3.33 Neighbor report response

6.3.33.1 General

The following MLME primitives support the signaling of neighbor report responses.

6.3.33.2.2 Semantics of the service primitive

The primitive parameters are as follows:

```
MLME-NEIGHBORREPRESP.request(
                             PeerSTAAddress,
                             DialogToken,
                             NeighborListSet,
                             VendorSpecificInfo
                             )
```

Source: 802.11 2016

Table 1: *802.11k Profile Parameters*

Parameter	Description
Advertise 802.11k Capability	Select this option to allow Virtual APs using this profile to advertise 802.11k capability. Default: Disabled
Forcefully disassociate on-hook voice clients	Select this option to allow the AP to forcefully disassociate *on-hook* voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its call admission control limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfill their QoS requirements. Default: Disabled
Measurement Mode for Beacon Reports	Click the **Measurement Mode for Beacon Reports** drop-down list and specify one of the following measurement modes: • **active-all-ch-**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. • **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. • **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. • **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table

Source:
https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm

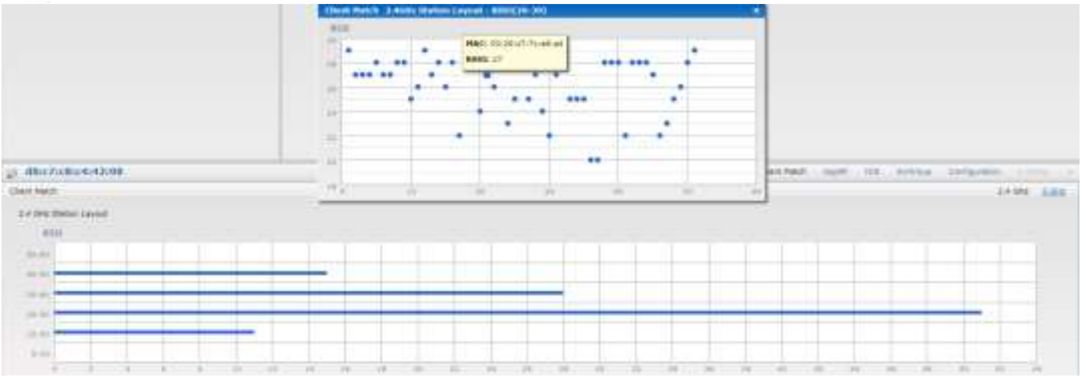
Client Match

If client match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.

The following figure shows the client distribution details for an AP radio.

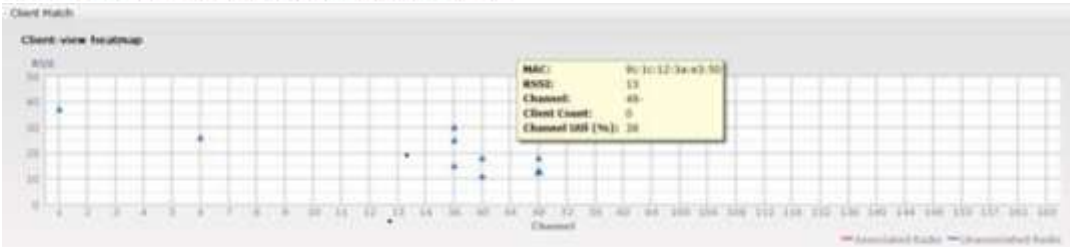
Figure 1 *Client Distribution on AP Radio*



On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

The following figure shows the client view heatmap for an AP radio:

Figure 2 *Channel Availability Map for Clients*



Source: https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Instant_user_interface/Client%20Match.htm

1. PC associates to AP-1. This becomes the PCs "Home AP"
2. All IAPs build a Virtual Beacon Report (VBR) with PC MAC, RSSI, band, etc, and uses this information to determine the "Best AP"
3. User picks up PC and moves closer to AP-3
4. The Home AP (AP-1) sends an "Adopt Request" to AP-2 and AP-3
5. Both AP-2 and AP-3 respond with an "Adopt Response" and AP-3 indicates it is the better choice based on RSSI and becomes the "Target AP"
6. AP-1 and AP-2 create Blacklist entries for the PC then AP-1 sends a de-auth to the PC
7. The only AP the PC can associate to is now AP-3. AP-1 and AP-2 will still hear the Probe Requests from the PC and use that in their VBR

- If the PC is "sticky" and does not want to be moved and it tries to associate back to AP-1 (8 attempts in 10 seconds) AP-1 will let it back in
- If the PC successfully moves to AP-3 no steering attempt will take place for 15 minutes

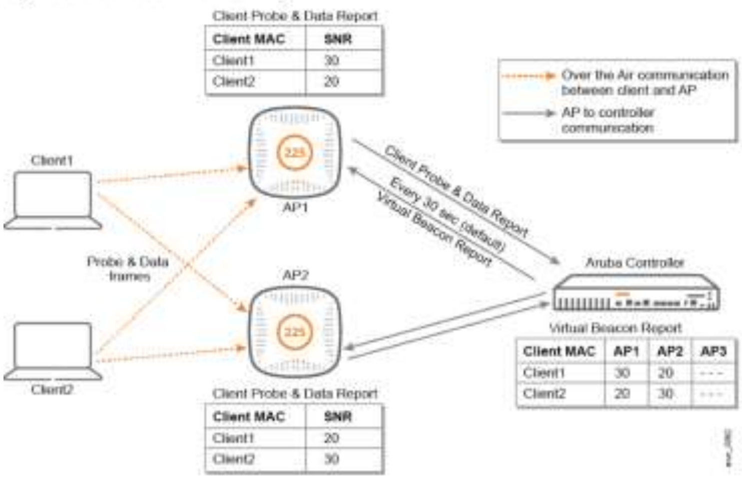
Source: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=22791

Selecting Optimal ClientMatch Settings

The ClientMatch figure shows how ClientMatch monitors each client's capabilities and connection on a WLAN using probe requests and data frames sent by the client.

- Each AP forms a client probe and data report, which includes a list of all the clients that an AP can hear, including the SNR.
- By default every 30 seconds APs send out this information to the controller, based on which a Virtual Beacon Report (VBR) is created, this maps each client to all the radios that can hear the client. Aruba controller sends out virtual beacon report of each client to the AP it is associated with.
- Based on the information received in the Virtual Beacon Report, an AP may decide to initiate band steering or sticky move for the clients associated to it. The decision to dynamically load balance the clients is however taken by the controller and not the APs.
- When a ClientMatch is initiated to move a client to the desired radio, all the radios in the RF vicinity except the one selected, blacklist the client for a short duration (default: 10 sec). This ensures that the client moves to the desired radio.

Figure 3 *ClientMatch Functionality*



Source: https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN

WLAN Configuration Profiles

Profile	Description
802.11k profile	The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. Each 802.11k profile also references one instance of each the following additional profile types. ■ Beacon Report Request profile: Defines beacon report request settings. Beacon report requests are sent only to 802.11k-compliant clients that advertise Beacon Report Capability in their Radio Resource Management Enabled Capabilities IE. ■ Radio Resource Management IE profile: Defines Radio Resource Management Information Elements for WLANs with 802.11k support enabled. ■ Traffic Stream Measurement Report Request profile: Defines Traffic Stream Measurement report requests. These report requests are sent only to 802.11k- compliant clients that advertise a traffic stream report capability. Default profile name: default

Source: https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/89/ArubaOS-8.9.0.0-User-Guide.pdf

Full interoperability with standards-based clients
ClientMatch uses industry standards such as 802.11k and 802.11v for its monitoring and control functions which ensures support for all client devices without additional software.

Source: https://www.arubanetworks.com/assets/tg/TB_EnhancedClientMatch.pdf

How ClientMatch Works
First, the clients associate to a radio. Next, all of the APs report probe requests from clients (as long as it's a good signal). If the client is 802.11k compliant, then the client informs the AP of other radios.

Then the controller builds a VBR (virtual beacon report) for ea ch client and shares this with the associated AP. The AP now has visibility into all available radios (APs) for this client. The AP now determines the optimum radio for this client.

Source: https://quizlet.com/433675597/ar-acma-8-dynamic-rf-management-flash-cards/

To allow the Instant AP and clients to exchange neighbor reports, ensure that Client Match is enablec through **RF > ARM > Client match > Enabled** in the WebUI or by executing the **client-match** command in the **arm** configuration sub-command mode.

Source:
https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/Instant_UG/WLAN_SSID_conf/Support%20for%20dot11r.htm#:

29. In the ’787 Accused Products, in response to the information indicating that a frequency channel is unavailable, the processor is configured to store information indicating that the frequency channel is unavailable from a set of frequency channels.

How ClientMatch Works
First, the clients associate to a radio. Next, all of the APs report probe requests from clients (as long as it's a good signal). If the client is 802.11k compliant, then the client informs the AP of other radios.

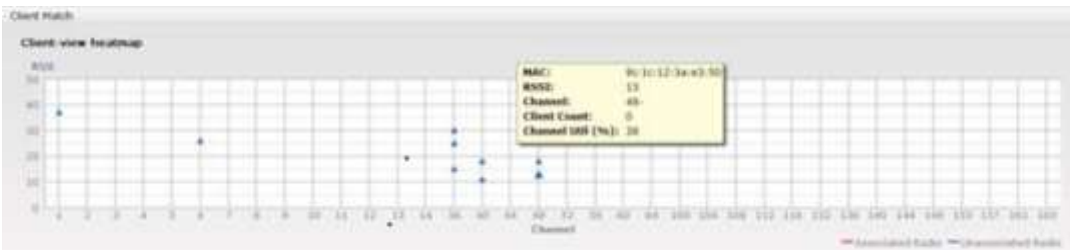
Then the controller builds a VBR (virtual beacon report) for ea ch client and shares this with the associated AP. The AP now has visibility into all available radios (APs) for this client. The AP now determines the optimum radio for this client.

Source: https://quizlet.com/433675597/ar-acma-8-dynamic-rf-management-flash-cards/

The ClientMatch figure shows how ClientMatch monitors each client's capabilities and connection on a WLAN using probe requests and data frames sent by the client.

- Each AP forms a client probe and data report, which includes a list of all the clients that an AP can hear, including the SNR.
- By default every 30 seconds APs send out this information to the controller, based on which a Virtual Beacon Report (VBR) is created, this maps each client to all the radios that can hear the client. Aruba controller sends out virtual beacon report of each client to the AP it is associated with.
- Based on the information received in the Virtual Beacon Report, an AP may decide to initiate band steering or sticky move for the clients associated to it. The decision to dynamically load balance the clients is however taken by the controller and not the APs.
- When a ClientMatch is initiated to move a client to the desired radio, all the radios in the RF vicinity except the one selected, blacklist the client for a short duration (default: 10 sec). This ensures that the client moves to the desired radio.

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN



Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Instant_user_interface/Client%20Match.htm

Aruba's Adaptive Radio Management™ (ARM) technology solves these challenges by dynamically choosing the best 802.11 channel and transmit power for each AP in the current RF environment. With ARM scanning enabled:

- Aruba APs dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but is not limited to neighboring APs' transmission power and channel, data regarding WLAN coverage, interference, and intrusion detection.
- ARM uses the information collected and calculates the channel quality for each channel in the spectrum and reports it back to the AP. Based on neighboring APs' transmission power, ARM also calculates coverage index.
- APs decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna or blocked signal from neighboring APs, each AP can effectively increase or decrease transmission power to provide sufficient coverage.

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN

Table 3: *Client Match Configuration Parameters*

Parameter	Description
Client match	Select **Enabled** to enable the **Client match** feature on APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview. By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled.

Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

Client Match

If client match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.

On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Instant_user_interface/Client%20Match.htm

When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an IAP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- **Dynamic Load Balancing**: Client match balances clients across IAPs on different channels, based on the client load on the IAPs and the SNR levels the client detects from an underutilized IAP. If an IAP radio can support additional clients, the IAP will participate in client match load balancing and clients can be directed to that IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

- **Channel Utilization**: Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**: Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.

Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

Radio Resource (802.11k) and BSS Transition Management (802.11v)

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports t each other. This allows the APs and clients to take appropriate connection actions.

The 802.11v BSS Transition capability can improve throughput, data rates and QoS for the voice clients in a network by shifting (via transition) the individual voice traffic loads to more appropriate points of association within the ESS.

Configuring the 802.11k Profile

The following procedures outline the steps to configure 802.11k parameters for a configuration node.

In the WebUI

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **System** > **Profiles** window.
2. In the Profiles list, expand the **Wireless LAN** menu, then select **802.11k**.
3. To edit an existing 802.11k profile, select the 802.1X profile you want to edit. To create a new 802.11k profile, click + and enter a name for the new 802.11k profile name in the **profile name** fiel
4. Configure your 802.11k radio settings. Table 1 outlines the parameters you can configure in the 802.11k profile.
5. Click **Save**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Table 1: *802.11k Profile Parameters*

Parameter	Description
Advertise 802.11k Capability	Select this option to allow Virtual APs using this profile to advertise 802.11k capability. Enabling this option also enables support for the 802.11v BSS transition management feature described in BSS Transition Management (802.11v). Default: Disabled
Measurement Mode for Beacon Reports	Click the **Measurement Mode for Beacon Reports** drop-down list and specify one of the following measurement modes: • **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. • **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. • **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. • **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table
Channel for Beacon Requests in 'A' band	This value is sent in the 'Channel' field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165. The default value is 36.
Channel for Beacon Requests in 'BG' band	This value is sent in the 'Channel' field of the Beacon Requests on the 'BG' radio. You can specify values in the range 1 to 14. The default value is 1.

Source: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm

- Dynamic Load Balancing—Client match balances clients across Instant APs on different channels, based on the client load on the Instant APs and the SNR levels the client detects from an underutilized Instant AP. If an Instant AP radio can support additional clients, the Instant AP will participate in client match load balancing and clients can be directed to that Instant AP radio, subjec to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

Source: https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

30. The '787 Accused Products further comprise the feature that, in response to the information indicating that the frequency channel is available, the processor is configured to

store information indicating that the frequency channel is available from the set of frequency channels.

How ClientMatch Works

First, the clients associate to a radio. Next, all of the APs report probe requests from clients (as long as it's a good signal). If the client is 802.11k compliant, then the client informs the AP of other radios.

Then the controller builds a VBR (virtual beacon report) for ea ch client and shares this with the associated AP. The AP now has visibility into all available radios (APs) for this client. The AP now determines the optimum radio for this client.

Source: https://quizlet.com/433675597/ar-acma-8-dynamic-rf-management-flash-cards/

The ClientMatch figure shows how ClientMatch monitors each client's capabilities and connection on a WLAN using probe requests and data frames sent by the client.

- Each AP forms a client probe and data report, which includes a list of all the clients that an AP can hear, including the SNR.
- By default every 30 seconds APs send out this information to the controller, based on which a Virtual Beacon Report (VBR) is created, this maps each client to all the radios that can hear the client. Aruba controller sends out virtual beacon report of each client to the AP it is associated with.
- Based on the information received in the Virtual Beacon Report, an AP may decide to initiate band steering or sticky move for the clients associated to it. The decision to dynamically load balance the clients is however taken by the controller and not the APs.
- When a ClientMatch is initiated to move a client to the desired radio, all the radios in the RF vicinity except the one selected, blacklist the client for a short duration (default: 10 sec). This ensures that the client moves to the desired radio.

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN

Aruba's Adaptive Radio Management™ (ARM) technology solves these challenges by dynamically choosing the best 802.11 channel and transmit power for each AP in the current RF environment. With ARM scanning enabled:

- Aruba APs dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but is not limited to neighboring APs' transmission power and channel, data regarding WLAN coverage, interference, and intrusion detection.
- ARM uses the information collected and calculates the channel quality for each channel in the spectrum and reports it back to the AP. Based on neighboring APs' transmission power, ARM also calculates coverage index.
- APs decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna or blocked signal from neighboring APs, each AP can effectively increase or decrease transmission power to provide sufficient coverage.

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN

Table 3: *Client Match Configuration Parameters*

Parameter	Description
Client match	Select **Enabled** to enable the **Client match** feature on APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview. By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled.

Source: https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

Measurement Mode for Beacon Reports	Click the **Measurement Mode for Beacon Reports** drop-down list and specify one of the following measurement modes: • **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. • **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. • **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. • **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table
Channel for Beacon Requests in 'A' band	This value is sent in the 'Channel' field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165. The default value is 36.
Channel for Beacon Requests in 'BG' band	This value is sent in the 'Channel' field of the Beacon Requests on the 'BG' radio. You can specify values in the range 1 to 14. The default value is 1.

Source: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm

Client Match

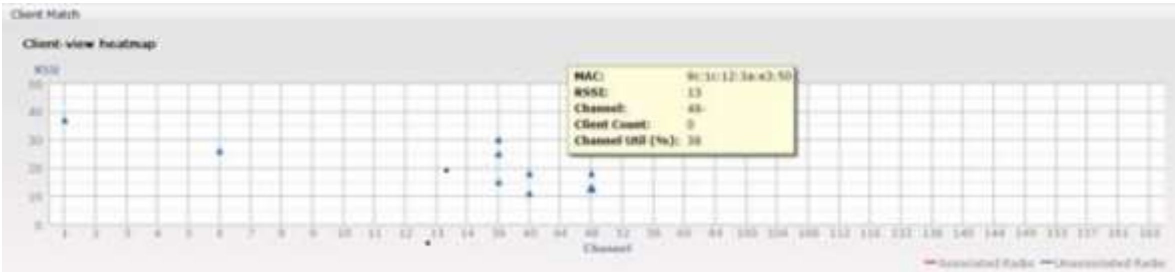
If client match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.

On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

The following figure shows the client view heatmap for an AP radio:

Figure 2 *Channel Availability Map for Clients*



Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Instant_user_interface/Client%20Match.htm

When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an IAP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- **Dynamic Load Balancing**: Client match balances clients across IAPs on different channels, based on the client load on the IAPs and the SNR levels the client detects from an underutilized IAP. If an IAP radio can support additional clients, the IAP will participate in client match load balancing and clients can be directed to that IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

- **Channel Utilization**: Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**: Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.

Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

- Dynamic Load Balancing—Client match balances clients across Instant APs on different channels, based on the client load on the Instant APs and the SNR levels the client detects from an underutilized Instant AP. If an Instant AP radio can support additional clients, the Instant AP will participate in client match load balancing and clients can be directed to that Instant AP radio, subjec to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

Source:
https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

31. In the '787 Accused Products the transceiver and the processor are configured to communicate using available frequency channels from the set of frequency channels.

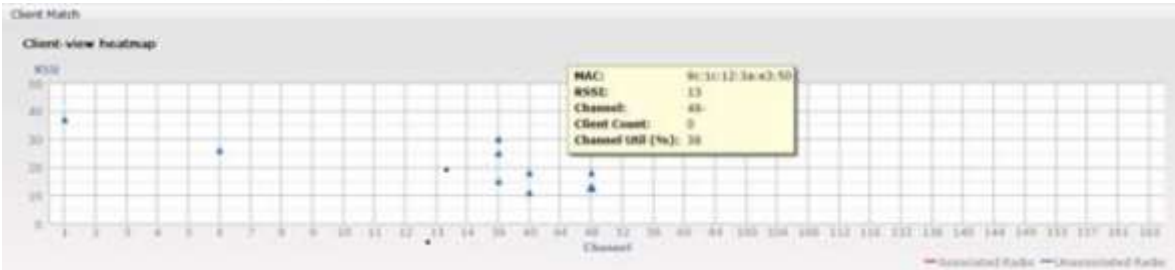
Client Match

If client match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual band, you can toggle between 2.4GHz and 5 GHz links in the client match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, client match status, and the client distribution on channels are displayed.

On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.
The following figure shows the client view heatmap for an AP radio:

Figure 2 *Channel Availability Map for Clients*



Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/Instant_user_interface/Client%20Match.htm

When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an IAP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- **Dynamic Load Balancing**: Client match balances clients across IAPs on different channels, based on the client load on the IAPs and the SNR levels the client detects from an underutilized IAP. If an IAP radio can support additional clients, the IAP will participate in client match load balancing and clients can be directed to that IAP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

- **Channel Utilization**: Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- **Client Capability Match**: Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.

Source:
https://www.arubanetworks.com/techdocs/Instant_41_Mobile/Advanced/Content/UG_files/ARM/Configuring_ARM-Features.htm

Selecting Optimal 802.11 Channel and Transmit Power

Selecting the right AP transmit power and channel helps improve the overall performance of the WLAN and provides better user experience. For example, if APs are operating on high power, then their coverage cells are large, resulting in co-channel and adjacent channel interference. Similar issues are observed if neighboring APs are operating on the same channel or an overlapping channel.

Aruba's Adaptive Radio Management™ (ARM) technology solves these challenges by dynamically choosing the best 802.11 channel and transmit power for each AP in the current RF environment. With ARM scanning enabled:

- Aruba APs dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but is not limited to neighboring APs' transmission power and channel, data regarding WLAN coverage, interference, and intrusion detection.
- ARM uses the information collected and calculates the channel quality for each channel in the spectrum and reports it back to the AP. Based on neighboring APs' transmission power, ARM also calculates coverage index.
- APs decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna or blocked signal from neighboring APs, each AP can effectively increase or decrease transmission power to provide sufficient coverage.

Channel

Though ARM takes care of selecting the appropriate channel for the APs, the following points should be considered as well:

- Since 802.11ac standard supports 80MHz channel boding, it can be used in Greenfield deployment (all 802.11ac access points). However, if 80MHz channel bonding needs to be used then U-NII-2A and U-NII-2C channels should be enabled to reduce adjacent channel and co-channel interference.
- Remove channel 144 from the list, as it is not supported by many devices.
- In high density open air environment, 20 or 40 MHz channel width helps in reducing channel utilization and improves overall network performance by providing more clear channels.

Addition of ARM Parameters

Free channel index - Value of this parameter helps ARM to select a new channel for an AP, which has been less utilized and has better quality. After scanning all channels, the AP calculates the **Interference Index** on its current channel and all other channels available on the same radio. If the AP traces another channel with the **Interference Index** value lesser than AP's current channel, it will move the AP to a new channel. The difference of total **Interference Index** between an AP's current channel and new channel should be equal to or more than the value defined by **Free Channel Index** (default value is 25).

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

- Dynamic Load Balancing—Client match balances clients across Instant APs on different channels, based on the client load on the Instant APs and the SNR levels the client detects from an underutilized Instant AP. If an Instant AP radio can support additional clients, the Instant AP will participate in client match load balancing and clients can be directed to that Instant AP radio, subjec to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.

Source:
https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

32. The processors of the ’787 Accused Products, which also support a feature called Adaptive Radio Management (“ARM”) determine a power level based on a received signal strength of the received wireless signal:

Selecting Optimal 802.11 Channel and Transmit Power

Selecting the right AP transmit power and channel helps improve the overall performance of the WLAN and provides better user experience. For example, if APs are operating on high power, then their coverage cells are large, resulting in co-channel and adjacent channel interference. Similar issues are observed if neighboring APs are operating on the same channel or an overlapping channel.

Aruba's Adaptive Radio Management™ (ARM) technology solves these challenges by dynamically choosing the best 802.11 channel and transmit power for each AP in the current RF environment. With ARM scanning enabled:

- Aruba APs dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but is not limited to neighboring APs' transmission power and channel, data regarding WLAN coverage, interference, and intrusion detection.
- ARM uses the information collected and calculates the channel quality for each channel in the spectrum and reports it back to the AP. Based on neighboring APs' transmission power, ARM also calculates coverage index.
- APs decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna or blocked signal from neighboring APs, each AP can effectively increase or decrease transmission power to provide sufficient coverage.

Channel

Though ARM takes care of selecting the appropriate channel for the APs, the following points should be considered as well:

- Since 802.11ac standard supports 80MHz channel boding, it can be used in Greenfield deployment (all 802.11ac access points). However, if 80MHz channel bonding needs to be used then U-NII-2A and U-NII-2C channels should be enabled to reduce adjacent channel and co-channel interference.
- Remove channel 144 from the list, as it is not supported by many devices.
- In high density open air environment, 20 or 40 MHz channel width helps in reducing channel utilization and improves overall network performance by providing more clear channels.

Addition of ARM Parameters

Free channel index - Value of this parameter helps ARM to select a new channel for an AP, which has been less utilized and has better quality. After scanning all channels, the AP calculates the **Interference Index** on its current channel and all other channels available on the same radio. If the AP traces another channel with the **Interference Index** value lesser than AP's current channel, it will move the AP to a new channel. The difference of total **Interference Index** between an AP's current channel and new channel should be equal to or more than the value defined by **Free Channel Index** (default value is 25).

Transmit Power

Although ARM alters AP's transmit power, there could still be instances when edge APs operate on maximum transmission power as they cannot hear neighboring APs and center APs could be operating on low transmission power due to the presence of too many neighbors.

- A difference of not more than 6 dB should be maintained between minimum and maximum transmit power within each ARM profile.
- A difference of 6 dB should be maintained between 802.11a and 802.11g radios, so that both bands have equal coverage and clients do not switch to 802.11g radio due to stronger signal strength.
- For 802.11ac APs that are deployed approximately 50 feet apart, the following minimum and maximum transmission power values are applicable :

Table 9: *Transmission Power Values*

	Open Office	Walled Office
A Radio Min Tx Power	12 dBm	15 dBm
A Radio Max Tx Power	15 dBm	18 dBm
G Radio Min Tx Power	6 dBm	6 dBm
G Radio Max Tx Power	9 dBm	9 dBm

NOTE

VoIP phones and badges have a restriction on the maximum transmission power they can support. Refer to the user manual or check the vendor's site and adjust APs transmit power accordingly.

NOTE

When there is no active user on the network, check the value of **channel busy** on Airwave or any other management tool. If the value is more than 30%, it indicates the presence of multiple beacons on the channel and co-channel interference could occur due to the AP's high transmit power.

NOTE

To efficiently control the RF characteristics of each band and implement the recommendations included in this guide, create separate ARM profiles and assign them to their individual Radio profiles.

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

Radio Resource Management (802.11k)

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions.

Table 1: *802.11k Profile Parameters*

Parameter	Description
Advertise 802.11k Capability	Select this option to allow Virtual APs using this profile to advertise 802.11k capability. Default: Disabled
Forcefully disassociate on-hook voice clients	Select this option to allow the AP to forcefully disassociate *on-hook* voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its call admission control limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfill their QoS requirements. Default: Disabled
Measurement Mode for Beacon Reports	Click the **Measurement Mode for Beacon Reports** drop-down list and specify one of the following measurement modes: • **active-all-ch-**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. • **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. • **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. • **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table

Source: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm

1. PC associates to AP-1. This becomes the PCs "Home AP"
2. All IAPs build a Virtual Beacon Report (VBR) with PC MAC, RSSI, band, etc, and uses this information to determine the "Best AP"
3. User picks up PC and moves closer to AP-3
4. The Home AP (AP-1) sends an "Adopt Request" to AP-2 and AP-3
5. Both AP-2 and AP-3 respond with an "Adopt Response" and AP-3 indicates it is the better choice based on RSSI and becomes the "Target AP"
6. AP-1 and AP-2 create Blacklist entries for the PC then AP-1 sends a de-auth to the PC
7. The only AP the PC can associate to is now AP-3. AP-1 and AP-2 will still hear the Probe Requests from the PC and use that in their VBR

- If the PC is "sticky" and does not want to be moved and it tries to associate back to AP-1 (8 attempts in 10 seconds) AP-1 will let it back in
- If the PC successfully moves to AP-3 no steering attempt will take place for 15 minutes

Source: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=22791

ARM Overview

ARM is an RF management technology that optimizes WLAN performance even in networks with the highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting pow for each Instant AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require

Source: https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

33. HPE has had knowledge of the ’787 patent since at least as early as the receipt of IV’s October 12, 2022 notice letter, which attached a copy of the ’787 patent, and will receive further knowledge by service upon HPE of the Complaint in this Case.

34. Additionally, HPE has been, and currently is, an active inducer of infringement of the ’787 patent under 35 U.S.C. § 271(b) and a contributory infringer of the ’787 patent under 35 U.S.C. § 271(c).

35. HPE has actively induced, and continues to actively induce, infringement of the ’787 patent by causing others to use, offer for sale, or sell products or services covered by the ’787 patent, including the ’787 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the ’787 patent. HPE’s inducement includes the directions and instructions found at:

- https://support.hpe.com/hpesc/public/docDisplay?docId=a00100446en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00062129en_us
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00073051en_us&docLocale=en_US

36. HPE has contributed to, and continues to contribute to, the infringement of the ’787 patent by others by selling the ’787 Accused Products, which, when installed, configured, and used directly infringe the ’787 patent.

37. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the ’787 patent.

38. HPE has committed, and continues to commit, contributory infringement by selling products and services that directly infringe the ’787 patent when used by a third party, such as the ’787 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the ’787 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

39. As a result of HPE’s acts of infringement, Intellectual Ventures II has suffered and will continue to suffer damages in an amount to be determined at trial.

COUNT II

(HPE’s Infringement of U.S. Patent No. RE44,706)

40. The preceding paragraphs are incorporated by reference.

41. The ’706 patent claims and teaches improved AP devices capable of transmitting and receiving identifiers corresponding to a service. In preferred embodiments, these identifiers may be included in 802.11ax Beacon frames. If a first AP receives an identifier transmitted by a second AP that identifies a service that is also offered by the first AP on the same radio channel (i.e., overlapping support for the service is detected), then the power of transmissions associated with that identified service can be reduced at the first AP if that service is also supported on the same radio channel by the first AP. A benefit of using APs of the invention is more efficient use

of wireless channels in a wireless network by reducing interference (i.e., the degree of overlap) between APs supporting the same service.

42. Prior art APs operating in device-dense environments did not advertise services that they support so that services could be differentiated by other APs, which in turn would allow those other APs to identify situations where an overlap in service (i.e., on the same radio channel) was being provided by the two APs. Without this capability, service overlap situations were not identified, which meant that the APs supporting the overlapping services could not reduce their transmit power so as not to interfere with one another. More specifically, claims of the ’706 patent recite an apparatus, e.g., an AP, for providing radio frequency access in support of at least one service to a client device. The apparatus may comprise a receiver operable to receive communications from the client device and to receive an RF identifier transmitted by another device, which may be another AP. The apparatus may include processing logic operable to determine whether the service associated with the received RF identifier is the same as a service supported by that AP, and to reduce the power of transmissions associated with that service (i.e., by the received RF identifier). The apparatus may further include a transmitter operable to transmit communications to the client device, the transmitter being further operable to support multiple services, and to transmit an RF domain identifier associated with each supported service.

43. HPE has directly infringed, and continues to directly infringe, at least claim 14 of the ’706 patent by making, using, selling, offering for sale, or importing products and services covered by claims of that patent. HPE’s products and services that infringe the ’706 patent include all APs that support mandatory provisions of the 802.11ax specification, such as the Aruba 500 Series Indoor Access Points, including the Aruba AP-505 Access Point, the Aruba

AP-515 Access Point, the AP-534 Access Point, the AP-535 Access Point, and the AP-555 Access Point, which are made, used, sold, or offered for sale by or on behalf of HPE (collectively, "the '706 Accused Products").

44. Claim 14 of the '706 patent is reproduced below:

14. A wireless access point comprising:

a transmitter configured to transmit a signal containing an identification of at least one service offered by the wireless access point; and

a receiver configured to receive from at least one other wireless access point at least one signal containing an identification of at least one service offered by the at least one other wireless access point;

wherein the wireless access point is configured:

to determine whether a received identification of at least one service offered by the at least one other wireless access point identifies at least one service also offered by the wireless access point, and,

to reduce a power level to be used by the transmitter to transmit at least signals associated with the at least one service also offered by the wireless access point, in the case where it is determined that the received identification of at least one service offered by the at least one other wireless access point identifies at least one service also offered by the wireless access point.

45. The '706 Accused Products include wireless access points:

Aruba 500 Series Indoor Access Points

Secure Wi-Fi 6 (802.11ax) access points for indoor environments such as mid-sized offices, schools, or retail spaces where fewer people are on the network at the same time.

Groundbreaking Wi-Fi 6 capabilities

Supports wired and wireless connectivity (in a single device) for up to 1.5 Gbps wireless and 256 associated clients per radio.

Source: https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/500-series/

46. The ’706 Accused Products comprise a transmitter configured to transmit a signal containing an identification of at least one service offered by the wireless access point. For example, each ’706 Accused Product (which is an AP) comprises radios that transmit Beacon frames containing an identification of a basic service set (“BSS”) and a BSS Color, which collectively enable other APs to place that BSS inside or outside a subset of BSSs supported by the network, which in turn allows another AP to identify overlapping BSS (“OBSS”) situations for that transmitted BSS. In an OBSS situation, the two APs are offering an overlapping BSS on the same channel, and as a result, it becomes desirable to take action to mitigate the interference and throughput effects of the OBSS situation.

Wi-Fi Radio Specifications

AP type: Indoor, dual radio, 5GHz and 2.4GHz 802.11ax 2x2 MIMO

5GHz radio: Two spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate with individual 2SS HE80 802.11ax client devices, or with two 1SS HE80 802.11a MU-MIMO capable client devices simultaneously

2.4GHz radio: Two spatial stream Single User (SU) MIMO for up to 574Mbps wireless data rate with individual 2SS HE40 802.11ax client devices or with two 1SS HE40 802.11ax MU-MIMO capable client devices simultaneously

Source: https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/500-series/

spatial reuse (SR): the transmission of a physical layer (PHY) protocol data unit (PPDU) on the medium under certain conditions when a PPDU has been detected that would otherwise have prevented the transmission.

spatial reuse group (SRG): A group of basic service sets (BSSs) identified by their BSS colors or partia basic service set identifiers (BSSIDs) for overlapping basic service set packet detect (OBSS PD)-based spa tial reuse operation with SRG OBSS PD level.

access point (AP): An entity that contains one station (STA) and provides access to the distribution systen services, via the wireless medium (WM) for associated STAs. An AP comprises a STA and a distributior system access function (DSAF).

station (STA): A logical entity that is a singly addressable instance of a medium access control (MAC) an physical layer (PHY) interface to the wireless medium (WM).

NOTE—For IEEE 802.11 purposes, a station is any MAC/PHY entity providing the IEEE 802.11 MAC services. Thi differs from the IEEE 802 definition of 'station,' which includes bridges (or 'end stations') that are endpoints of linl layer data traffic.

Source: 802.11ax-2021

4.3.4 STA membership in a BSS is dynamic

A STA's membership in a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range). To become a member of an infrastructure BSS or an IBSS, a STA joins the BSS using the synchronization procedure described in 11.1.4.5. To start a new mesh BSS or to become a member of a mesh BSS, a STA starts the transmission of Beacon frames and performs the synchronization maintenance procedure described in 14.13. To access all of the services of an infrastructure BSS, a STA becomes "associated." These associations are dynamic and involve the use of the distribution system service (DSS), which is describe in 4.4.4. A mesh STA does not become associated as there is no central entity in a mesh BSS (MBSS)

Figure 4-2 adds the DS, DSM, and AP components to the IEEE 802.11 architecture picture.

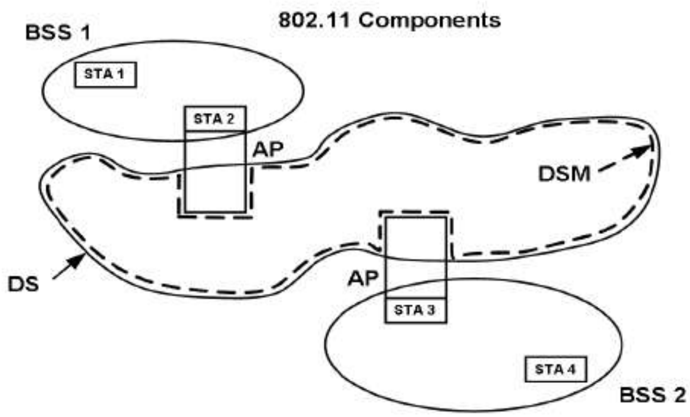


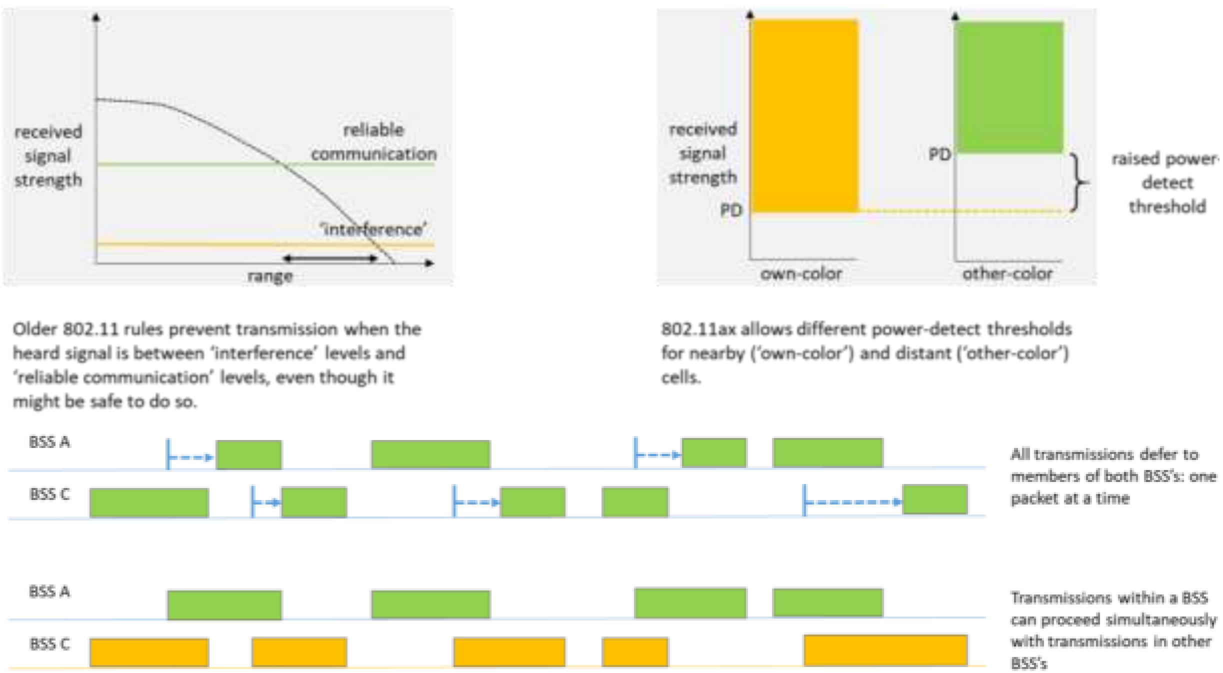
Figure 4-2—DSs and APs

basic service set (BSS): A set of stations (STAs) that have successfully synchronized using the JOIN service primitives[17] and one STA that has used the START primitive. Alternatively, a set of STAs that have used the START primitive specifying matching mesh profiles where the match of the mesh profiles has been verified via the scanning procedure. Membership in a BSS does not imply that wireless communication with all other members of the BSS is possible.

transmitted basic service set identifier (BSSID): The BSSID included in the medium access control (MAC) header transmitter address field of a Beacon frame when the multiple BSSID capability is supported.

Source: 802.11ax-2021

One focus of the next Wi-Fi standard, 802.11ax (also known as Wi-Fi 6), is to improve the performance of 'real-world' networks, and to this end, the new standard includes a feature enabling more simultaneous transmissions. This feature is known as 'spatial reuse' or 'BSS coloring'.



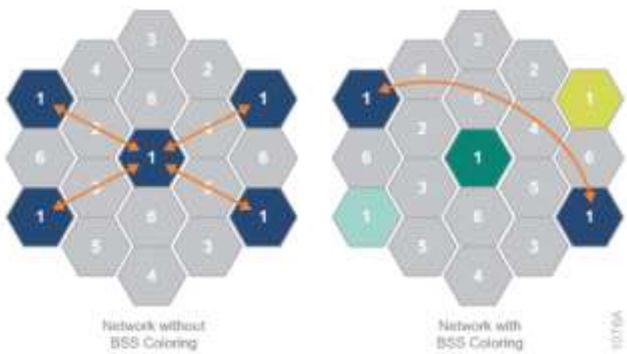
BSS coloring: before and after

Source: https://blogs.arubanetworks.com/corporate/extending-network-capacity-in-enterprise-wlans-with-802-11/

BSS Coloring

BSS coloring allows the network to assign a "color" tag to a channel and reduce the threshold for interference. Network performance is improved because APs on the same channel can be closer together and still transmit at the same time as long as they are different colors. Because we can have fewer channels, it may also be possible for organizations to use wider channels, such as 80Mhz channels in some or all of their network.

Figure 7 *Left—without BSS coloring, all overlapping channels interfere.*
Right—with BSS coloring, only matching colors interfere.



Source: https://www.arubanetworks.com/assets/wp/WP_Multi-User-802.11ax.pdf

9.3.3.2 Beacon frame format

Change the following rows in Table 9-34 (Beacon frame body) maintaining row order:

Table 9-34—Beacon frame body

		mented is true; otherwise it is not present.
78	HE Operation	The HE Operation element is present if dot11HEOptionImplemented is true; otherwise it is not present.

9.4.2.248 HE Operation element

The operation of HE STAs in an HE BSS is controlled by the following:

— the HT Operation element and the HE Operation element if operating in the 2.4 GHz band

— the HT Operation element, VHT Operation element (if present) and the HE Operation element if operating in the 5 GHz band

— The HE Operation element if operating in the 6 GHz band

The format of the HE Operation element is defined in Figure 9-787h (HE Operation element format).

Element ID	Length	Element ID Extension	HE Operation Parameters	BSS Color Information	Basic HE-MCS And NSS Set	VHT Operation Information	Max Co-Hosted BSSID Indicator	6 GHz Operation Information
Octets: 1	1	1	3	1	2	0 or 3	0 or 1	0 or 5

Figure 9-787h—HE Operation element format

Source: 802.11ax-2021

47. The ’706 Accused Products include a receiver configured to receive from at least one other wireless AP at least one signal containing an identification of at least one service offered by the other wireless AP. For example, ’706 Accused Products implementing 802.11ax include radios configured to receive Beacon frames from neighboring APs. Beacon frames comprise an identification of services offered by the APs, including the BSS and BSS color.

Wi-Fi Radio Specifications

AP type: Indoor, dual radio, 5GHz and 2.4GHz 802.11ax 2x2 MIMO

5GHz radio: Two spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate with individual 2SS HE80 802.11ax client devices, or with two 1SS HE80 802.11a MU-MIMO capable client devices simultaneously

2.4GHz radio: Two spatial stream Single User (SU) MIMO for up to 574Mbps wireless data rate with individual 2SS HE40 802.11ax client devices or with two 1SS HE40 802.11ax MU-MIMO capable client devices simultaneously

Source: https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/500-series/

9.3.3.2 Beacon frame format

Table 9-32—Beacon frame body

Table 9-32—Beacon frame body *(continued)*

Order	Information	Notes
67	Common Advertisement Group (CAG) Number	The CAG Number element is optionally present if dot11FILSActivated is true; otherwise not present.
68	FILS Indication	The FILS Indication element is present if dot11FILSActivated is true; otherwise not present.
69	AP-CSN	The AP Configuration Sequence Number (AP-CSN) element is optionally present if dot11FILSActivated is true; otherwise not present.
70	DILS	The DILS element is optionally present if dot11FILSActivated is true; otherwise not present.
71	Max Channel Switch Time	The Max Channel Switch Time element is optionally present when a Channel Switch Announcement or an Extended Channel Switch Announcement element is also present.
72	Estimated Services Parameters Outbound	The Estimated Service Parameters Outbound element is optionally present if dot11EstimatedServiceParametersOutboundOptionImplemented is true.
73	Service Hint	The Service Hint element is optionally present if dot11UnsolicitedPADActivated is true.
74	Service Hash	The Service Hash element is optionally present if dot11UnsolicitedPADActivated is true.
75	RSN Extension	The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.
Last -1	Vendor Specific	One or more Vendor Specific elements are optionally present. These elements follow all other elements.
Last	MME	The MME is present if dot11BeaconProtectionEnabled is true at the AP.
NOTE—The MME appears after all fields that it protects. Therefore, it appears last in the frame body to protect the frames as specified in 12.5.4.		

Table 9-34—Beacon frame body

78	HE Operation	The HE Operation element is present if dot11HEOptionImplemented is true; otherwise it is not present.

9.4.2.248 HE Operation element

The operation of HE STAs in an HE BSS is controlled by the following:

— the HT Operation element and the HE Operation element if operating in the 2.4 GHz band

— the HT Operation element, VHT Operation element (if present) and the HE Operation element if operating in the 5 GHz band

— The HE Operation element if operating in the 6 GHz band

The format of the HE Operation element is defined in Figure 9-787h (HE Operation element format).

	Element ID	Length	Element ID Extension	HE Operation Parameters	BSS Color Information	Basic HE-MCS And NSS Set	VHT Operation Information	Max Co-Hosted BSSID Indicator	6 GHz Operation Information
Octets:	1	1	1	3	1	2	0 or 3	0 or 1	0 or 5

Figure 9-787h—HE Operation element format

Source: 802.11ax-2021

3. **Multiuser capabilities with spatial reuse** – For a long time, the main problem with Wi-Fi has been that the signals go too far, and that causes interference. Spatial reuse, or BSS coloring, resolves this challenge. BSS coloring increases the capacity for congested environments where there are overlapping APs, and it results in a 2x capacity over 802.11ax.

With the introduction of BSS coloring, packets from different devices now can be on the same channel at the same time. They no longer have to wait for each other to finish, which means more bits can be transmitted in the same amount of time.

With BSS coloring, each AP and cell has an assigned color, and the behavior can be different when an AP has the same or different color than the client. If the colors don't match, then the original power settings are used. But if the colors do match, a higher set of power thresholds can be used, so they can transmit on top of the other client.

For example, say Bob and Alice are in a building, and an AP on the west side is transmitting to Bob's phone. An AP in the east corner is transmitting to Alice's laptop. The power level of the AP on the west side is weak, but still audible. In the old days, the AP on Bob's side wouldn't transmit when it could still hear the signal. But now with colors assigned to the APs on the east and west sides, when the signal is transmitted to the other side, the other AP knows that it's a different color and thus won't interfere. It doesn't need to wait for the other transmission to complete before starting its own transmission. This capability is built into the AP, so there's nothing the user or client needs to do.

Source: https://www.networkworld.com/article/3337236/6-ways-802-11ax-gives-you-better-wi-fi-experience.html

26.2.2 Intra-BSS and inter-BSS PPDU classification

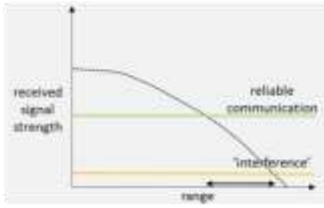
A STA shall classify a received PPDU as an inter-BSS PPDU if at least one of the following conditions is true:

— The RXVECTOR parameter BSS_COLOR is not 0 and is not the BSS color of the BSS of which the STA is a member.

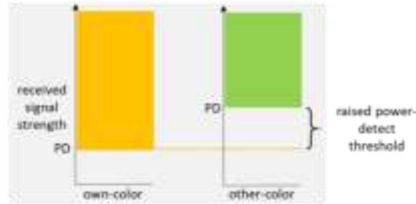
Source: 802.11ax-2021

Better Spatial Reuse with BSS Coloring

Traditional Wi-Fi uses a single CCA power-detect value based on the power level of a packet on the air to determine if it is 'clear'. 802.11ax allows for two values, one for access points and their clients that are nearby (currently -82 dBm) and others for more distant cells (probably -62 dBm), the idea being that distant cells will not be affected by interference from a local transmission.



Older 802.11 rules prevent transmission when the heard signal is between 'interference' levels and 'reliable communication' levels, even though it might be safe to do so.



802.11ax allows different power-detect thresholds for nearby ('own-color') and distant ('other-color') cells.

The definition of a nearby access point is one with a different 'color' tag in its and its clients' transmissions. The tag is added to the 802.11ax preamble: 6 bits are allocated for 63 possible values. When a network is colored correctly, cells at different ends of a building – which would previously have deferred to each other's CCA, so only one could transmit at any time – will be able to transmit simultaneously, without incurring higher retransmissions and error rates.

BSS coloring: before and after

The change in power-detect threshold is linked to transmit power control, ensuring that the power used is just sufficient to reach the intended receiver, and no more. And it may be linked to RTS-CTS (Request-to-Send, Clear-to-Send) to clear the channel for the transmission: but these are details, the significant improvement is due to dynamic power-detect thresholds.

Source: https://blogs.arubanetworks.com/corporate/extending-network-capacity-in-enterprise-wlans-with-802-11/

Spatial Reuse Channel Access Rules

- BOTH the AP and clients can now differentiate between intra-BSS frames and OBSS frames with use of BSS Color bits and apply less sensitive CCA threshold to OBSS frames
  - Higher CCA value leads to more simultaneous transmissions, but potentially lowers SINR
  - The goal is to increase the reuse, while not causing a significant reduction to selected MCS due to interference
- Adaptive CCA
  - 802.11 signal detect and TXPWR threshold may be adjusted dynamically by both AP and clients

Source: https://hobbydocbox.com/Radio/107575371-802-11ax-and-ad-sneak-peek.html

48. The ’706 Accused Products comprise a feature in which the wireless AP is configured to determine whether a received identification of a service offered by another wireless AP identifies a service also offered by the first wireless AP. For example, the Beacon frame may contain an identification of services offered by the other wireless AP, using BSS coloring, that may also be offered by the first wireless AP.

3. **Multiuser capabilities with spatial reuse –** For a long time, the main problem with Wi-Fi has been that the signals go too far, and that causes interference. Spatial reuse, or BSS coloring, resolves this challenge. BSS coloring increases the capacity for congested environments where there are overlapping APs, and it results in a 2x capacity over 802.11ax.

With the introduction of BSS coloring, packets from different devices now can be on the same channel at the same time. They no longer have to wait for each other to finish, which means more bits can be transmitted in the same amount of time.

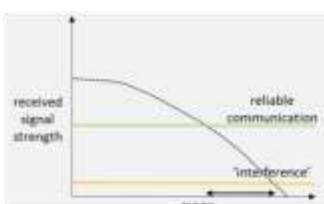
With BSS coloring, each AP and cell has an assigned color, and the behavior can be different when an AP has the same or different color than the client. If the colors don't match, then the original power settings are used. But if the colors do match, a higher set of power thresholds can be used, so they can transmit on top of the other client.

For example, say Bob and Alice are in a building, and an AP on the west side is transmitting to Bob's phone. An AP in the east corner is transmitting to Alice's laptop. The power level of the AP on the west side is weak, but still audible. In the old days, the AP on Bob's side wouldn't transmit when it could still hear the signal. But now with colors assigned to the APs on the east and west sides, when the signal is transmitted to the other side, the other AP knows that it's a different color and thus won't interfere. It doesn't need to wait for the other transmission to complete before starting its own transmission. This capability is built into the AP, so there's nothing the user or client needs to do.

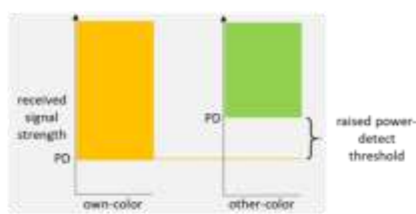
Source: https://www.networkworld.com/article/3337236/6-ways-802-11ax-gives-you-better-wi-fi-experience.html

Better Spatial Reuse with BSS Coloring

Traditional Wi-Fi uses a single CCA power-detect value based on the power level of a packet on the air to determine if it is 'clear'. 802.11ax allows for two values, one for access points and their clients that are nearby (currently -82 dBm) and others for more distant cells (probably -62 dBm), the idea being that distant cells will not be affected by interference from a local transmission.

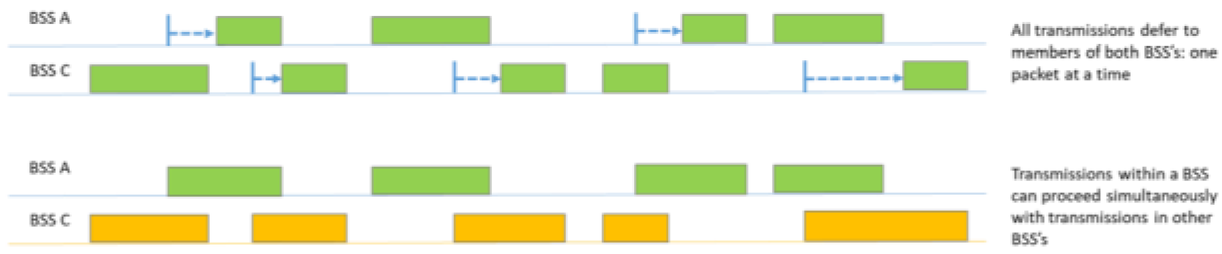


Older 802.11 rules prevent transmission when the heard signal is between 'interference' levels and 'reliable communication' levels, even though it might be safe to do so.



802.11ax allows different power-detect thresholds for nearby ('own-color') and distant ('other-color') cells.

The definition of a nearby access point is one with a different 'color' tag in its and its clients' transmissions. The tag is added to the 802.11ax preamble: 6 bits are allocated for 63 possible values. When a network is colored correctly, cells at different ends of a building – which would previously have deferred to each other's CCA, so only one could transmit at any time – will be able to transmit simultaneously, without incurring higher retransmissions and error rates.



BSS coloring: before and after

The change in power-detect threshold is linked to transmit power control, ensuring that the power used is just sufficient to reach the intended receiver, and no more. And it may be linked to RTS-CTS (Request-to-Send, Clear-to-Send) to clear the channel for the transmission: but these are details, the significant improvement is due to dynamic power-detect thresholds.

Source: https://blogs.arubanetworks.com/corporate/extending-network-capacity-in-enterprise-wlans-with-802-11/

26.2.2 Intra-BSS and inter-BSS PPDU classification

A STA shall classify a received PPDU as an inter-BSS PPDU if at least one of the following conditions is true:

— The RXVECTOR parameter BSS_COLOR is not 0 and is not the BSS color of the BSS of which the STA is a member.

A STA shall classify the received PPDU as an intra-BSS PPDU if at least one of the following conditions is true:

— The RXVECTOR parameter BSS_COLOR of the PPDU carrying the frame is the BSS color of the BSS of which the STA is a member or the BSS color of any TDLS links to which the STA belongs if the STA is an HE STA associated with a non-HE AP.

Source: 802.11ax-2021

Spatial Reuse Channel Access Rules

– BOTH the AP and clients can now differentiate between intra-BSS frames and OBSS frames with use of BSS Color bits and apply less sensitive CCA threshold to OBSS frames

  – Higher CCA value leads to more simultaneous transmissions, but potentially lowers SINR

  – The goal is to increase the reuse, while not causing a significant reduction to selected MCS due to interference

– Adaptive CCA

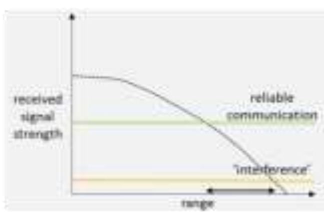
  – 802.11 signal detect and TXPWR threshold may be adjusted dynamically by both AP and clients

Source: https://hobbydocbox.com/Radio/107575371-802-11ax-and-ad-sneak-peek.html

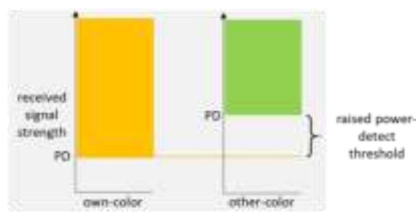
49. The ’706 Accused Products are further configured to reduce a power level to be used by the transmitter to transmit signals associated with the service also offered by the other wireless AP, where it is determined that the received identification of the service offered by the other wireless AP identifies a service also offered by the first wireless AP. For example, where two APs offer OBSSs, the transmitting AP will not be as reliant on the CSMA/CD protocol to share the wireless medium (i.e., by using a lower CCA power detect threshold, that if met causes an AP to delay its transmission until other APs operating on the same channel have completed their transmissions), and will instead reduce its transmit power level to better coexist (without excessive interference) with the other AP operating in an OBSS (i.e., as the power detect threshold is raised for the CSMA/CD protocol in place for these two APs supporting the OBSS).

Better Spatial Reuse with BSS Coloring

Traditional Wi-Fi uses a single CCA power-detect value based on the power level of a packet on the air to determine if it is 'clear'. 802.11ax allows for two values, one for access points and their clients that are nearby (currently -82 dBm) and others for more distant cells (probably -62 dBm), the idea being that distant cells will not be affected by interference from a local transmission.



Older 802.11 rules prevent transmission when the heard signal is between 'interference' levels and 'reliable communication' levels, even though it might be safe to do so.



802.11ax allows different power-detect thresholds for nearby ('own-color') and distant ('other-color') cells.

The definition of a nearby access point is one with a different 'color' tag in its and its clients' transmissions. The tag is added to the 802.11ax preamble: 6 bits are allocated for 63 possible values. When a network is colored correctly, cells at different ends of a building – which would previously have deferred to each other's CCA, so only one could transmit at any time – will be able to transmit simultaneously, without incurring higher retransmissions and error rates.

BSS coloring: before and after

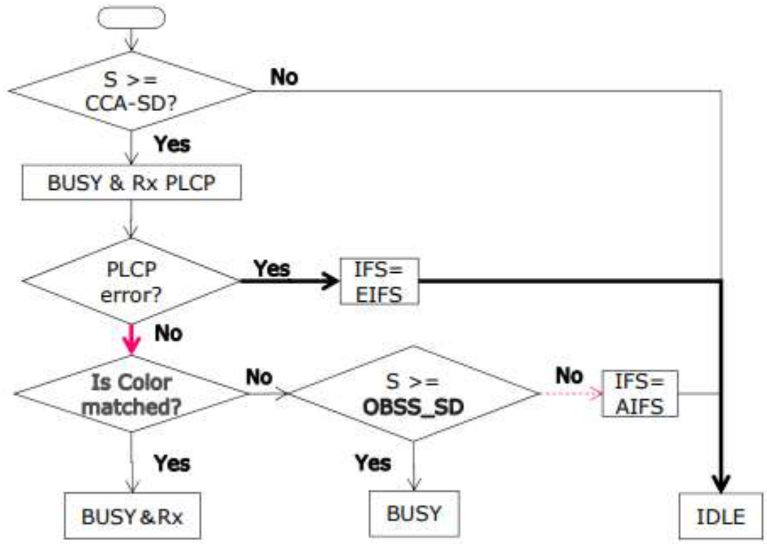
The change in power-detect threshold is linked to transmit power control, ensuring that the power used is just sufficient to reach the intended receiver, and no more. And it may be linked to RTS-CTS (Request-to-Send, Clear-to-Send) to clear the channel for the transmission: but these are details, the significant improvement is due to dynamic power-detect thresholds.

Source: https://blogs.arubanetworks.com/corporate/extending-network-capacity-in-enterprise-wlans-with-802-11/

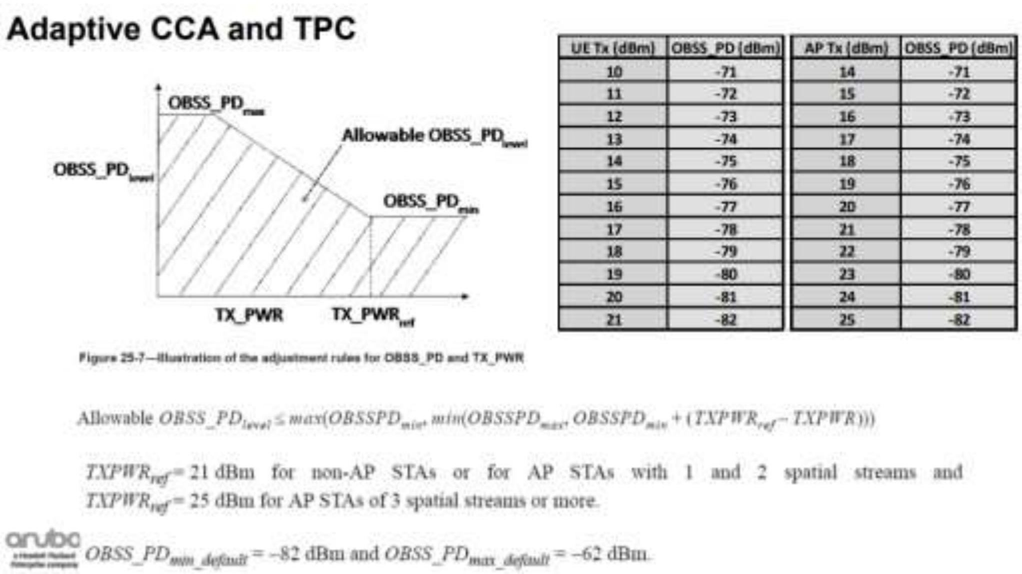
Spatial Reuse Channel Access Rules

– BOTH the AP and clients can now differentiate between intra-BSS frames and OBSS frames with use of BSS Color bits and apply less sensitive CCA threshold to OBSS frames
  – Higher CCA value leads to more simultaneous transmissions, but potentially lowers SINR
  – The goal is to increase the reuse, while not causing a significant reduction to selected MCS due to interference
– Adaptive CCA
  – 802.11 signal detect and TXPWR threshold may be adjusted dynamically by both AP and clients

Source: https://hobbydocbox.com/Radio/107575371-802-11ax-and-ad-sneak-peek.html



Source: https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=042c0bdb-5120-4f50-9d43-1ed4514c324f



UE Tx (dBm)	OBSS_PD (dBm)	AP Tx (dBm)	OBSS_PD (dBm)
10	-71	14	-71
11	-72	15	-72
12	-73	16	-73
13	-74	17	-74
14	-75	18	-75
15	-76	19	-76
16	-77	20	-77
17	-78	21	-78
18	-79	22	-79
19	-80	23	-80
20	-81	24	-81
21	-82	25	-82

Source: https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=042c0bdb-5120-4f50-9d43-1ed4514c324f

50. HPE has had knowledge of the ’706 patent since at least as early as the receipt of IV’s October 12, 2022 notice letter, which attached a copy of the ’706 patent, and will receive further knowledge by service upon HPE of the Complaint in this Case.

51. Additionally, HPE has been, and currently is, an active inducer of infringement of the ’706 patent under 35 U.S.C. § 271(b) and a contributory infringer of the ’706 patent under 35 U.S.C. § 271(c).

52. HPE has actively induced and continues to actively induce infringement of the ’706 patent by causing others to use, offer for sale, or sell, products or services covered by the ’706 patent, including the ’706 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the ’706 patent. HPE’s inducement includes the directions and instructions found at:

- https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=042c0bdb-5120-4f50-9d43-1ed4514c324f
- https://blogs.arubanetworks.com/corporate/extending-network-capacity-in-enterprise-wlans-with-802.11/
- https://www.arubanetworks.com/assets/wp/WP_Multi-User-802.11ax.pdf
- https://www.arubanetworks.com/techdocs/ArubaOS_83_Web_Help/Content/ArubaFrameStyles/AP_Config/rf_mgmnt_2.4_5_ghz_radio_supprt_add_rf_mgmt_ui.htm
- https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/virtual-ap/adva-hith-radi-sett.htm
- https://www.arubanetworks.com/techdocs/Instant_89_WebHelp/Content/instant-ug/arm/conf-radio-sett.htm
- https://www.arubanetworks.com/techdocs/CLI-Bank/Content/aos8/rf-ht-rad-pro.htm

53. HPE has contributed to and continues to contribute to the infringement of the ’706 patent by others by selling the ’706 Accused Products, which, when installed, configured, and used directly infringe the ’706 patent.

54. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the ’706 patent.

55. HPE has committed and continues to commit contributory infringement by selling products and services that directly infringe the ’706 patent when used by a third party, such as the ’706 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the ’706 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

56. As a result of HPE’s acts of infringement, Intellectual Ventures II has suffered and will continue to suffer damages in an amount to be determined at trial.

COUNT III

(HPE’s Infringement of U.S. Patent No. 7,623,439)

57. The preceding paragraphs are incorporated by reference.

58. The ’439 patent claims and teaches an improved signal transmitting system capable of manipulating orthogonal frequency division multiplexed (“OFDM”) data packets and data streams using improved cyclic diversity schemes, thereby improving packet reception performance when compared to conventional packet diversity mechanisms by reducing packet error rates, among other benefits.

59. In the prior art, cyclic diversity schemes (e.g., the cyclic-delay diversity scheme), two or more transmitters send the same data in a spatial stream, but cyclically offset one spatial stream vis a vis the other using a delay interval. Such systems relied on relatively small cyclic delays. By introducing a relatively small cyclic delay to the transmitted diversity signal (as compared to the original transmitted signal on which the diversity signal is based) however, the

symbol data portions of the two different transmitted signals cannot be easily decorrelated, thus reducing the probability of unintentional beamforming . More specifically, claims of the ’439 patent recite a method for transmitting OFDM signals. The method comprises generating a first OFDM packet for transmission including a guard interval portion and a symbol data portion, each comprised of a plurality of samples. The method further comprises cyclically advancing the first OFDM packet by shifting the samples in a first direction an amount less than a sample duration of the guard interval portion to generate a shifted version of the first OFDM packet for transmission in which samples from the symbol data portion of the first OFDM packet are shifted into the guard interval portion of the shifted version and the same number of samples from the guard interval portion of the first OFDM packet are shifted out of the guard interval portion of the shifted version, and substantially simultaneously transmitting the first OFDM packet and the shifted version of the OFDM packet.

60. HPE has directly infringed and continues to directly infringe at least claim 1 of the ’439 patent by making, using, selling, offering for sale, or importing products and services covered by the claims of that patent. HPE’s products or services that infringe the ’439 patent include all wireless communication products that support IEEE 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), or 802.11ax (Wi-Fi 6), including the transmission of multiple spatial streams, which requires the cyclic diversity shift when transmitting OFDM packets, including the Aruba 203H, Aruba 303H, Aruba 318, Aruba 370, and Aruba 500 lines of APs that are made, used, sold, or offered for sale by or on behalf of HPE (cumulatively, “the ’439 Accused Products”).

61. Claim 1 of the ’439 patent is reproduced below:

1. A method for transmitting orthogonal frequency division multiplexing (OFDM) signals comprising:

generating a first OFDM packet for transmission including a guard interval portion and a symbol data portion each comprised of a plurality of samples;

cyclically advancing the first OFDM packet by shifting the samples in a first direction an amount less than a sample duration of the guard interval portion to generate a shifted version of the first OFDM packet for transmission in which at least a non-zero number of the samples from the symbol data portion of the first OFDM packet are shifted into the guard interval portion of the shifted version and a same non-zero number of samples from the guard interval portion of the first OFDM packet are shifted out of the guard interval portion of the shifted version; and

substantially simultaneously transmitting the first OFDM packet and the shifted version of the OFDM packet.

62. The '439 Accused Products are configured to perform a method for transmitting OFDM signals. As one example, the Aruba 370 supports OFDM:

Aruba 370 - Product Information Reference

Table 1: WI-FI radio specifications

Specifications	**Description**
AP type	Outdoor hardened, dual radio, 5 GHz 802.11ac 4 x 4 MIMO and 2.4 GHz 802.11n 2 x 2 MIMO
Supported radio technologies	• 802.11b: Direct-Sequence Spread-Spectrum (DSSS) • 802.11a/g/n/ac: Orthogonal Frequency-Division Multiplexing (OFDM)
Cyclic Delay/Shift Diversity (CDD/CSD)	Improved downlink RF performance
Short guard interval	20 MHz, 40 MHz, 80 MHz and 160 MHz channels

Souce:
https://support.hpe.com/hpesc/public/docDisplay?docId=a00030293en_us&docLocale=en_US&page=GUID-CF0ADA95-49A9-4A7A-A609-EF4D39420C3A.html

63. The method practiced by the '439 Accused Products includes generating a first OFDM packet for transmission including a guard interval portion and a symbol data portion each comprised of a plurality of samples:

20. High Throughput (HT) PHY specification

20.1 Introduction

20.1.1 Introduction to the HT PHY

Clause 20 specifies the PHY entity for a high throughput (HT) orthogonal frequency division multiplexing (OFDM) system.

In addition to the requirements found in Clause 20, an HT STA shall be capable of transmitting and receiving frames that are compliant with the mandatory PHY specifications defined as follows:

— In Clause 18 when the HT STA is operating in a 20 MHz channel width in the 5 GHz band

— In Clause 17 and Clause 19 when the HT STA is operating in a 20 MHz channel width in the 2.4 GHz band

The HT PHY is based on the OFDM PHY defined in Clause 18, with extensibility up to four spatial streams, operating in 20 MHz bandwidth. Additionally, transmission using one to four spatial streams is defined for operation in 40 MHz bandwidth. These features are capable of supporting data rates up to 600 Mb/s (four spatial streams, 40 MHz bandwidth).

The HT PHY data subcarriers are modulated using binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), 16-quadrature amplitude modulation (16-QAM), or 64-QAM. Forward error correction (FEC) coding (convolutional coding) is used with a coding rate of 1/2, 2/3, 3/4, or 5/6. LDPC codes are added as an optional feature.

Source: IEEE Std 802.11-2012

20.1.2 Scope

The services provided to the MAC by the HT PHY consist of two protocol functions, defined as follows:

a) A PHY convergence function, which adapts the capabilities of the physical medium dependent (PMD) system to the PHY service. This function is supported by the physical layer convergence procedure (PLCP), which defines a method of mapping the PSDUs into a framing format (PPDU) suitable for sending and receiving PSDUs between two or more STAs using the associated PMD system.

Source: IEEE Std 802.11-2012

20.1.4 PPDU formats

The structure of the PPDU transmitted by an HT STA is determined by the TXVECTOR FORMAT, CH_BANDWIDTH, CH_OFFSET, and MCS parameters as defined in Table 20-1. The effect of the CH_BANDWIDTH, CH_OFFSET, and MCS parameters on PPDU format is described in 20.2.3.

The FORMAT parameter determines the overall structure of the PPDU as follows:

— *Non-HT format* **(NON_HT):** Packets of this format are structured according to the Clause 18 (OFDM) or Clause 19 (ERP) specification. Support for non-HT format is mandatory.

— *HT-mixed format* **(HT_MF):** Packets of this format contain a preamble compatible with Clause 18 and Clause 19 receivers. The non-HT-STF (L-STF), the non-HT-LTF (L-LTF), and the non-HT SIGNAL field (L-SIG) are defined so they can be decoded by non-HT Clause 18 and Clause 19 STAs. The rest of the packet cannot be decoded by Clause 18 or Clause 19 STAs. Support for HT-mixed format is mandatory.

— *HT-greenfield format* **(HT_GF):** HT packets of this format do not contain a non-HT compatible part. Support for HT-greenfield format is optional. An HT STA that does not support the reception of an HT-greenfield format packet shall be able to detect that an HT-greenfield format packet is an HT transmission (as opposed to a non-HT transmission). In this case, the receiver shall decode the HT-SIG and determine whether the HT-SIG cyclic redundancy check (CRC) passes.

Source: IEEE Std 802.11-2012

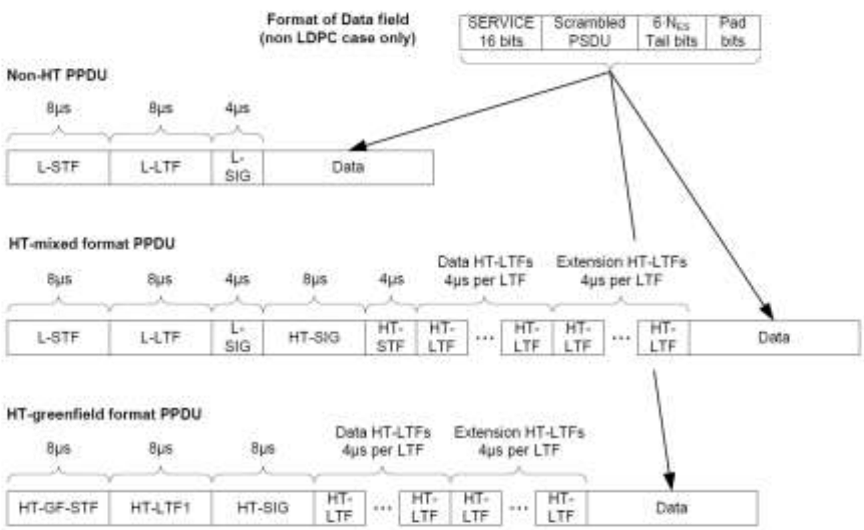


Figure 20-1—PPDU format

Source: IEEE Std 802.11-2012

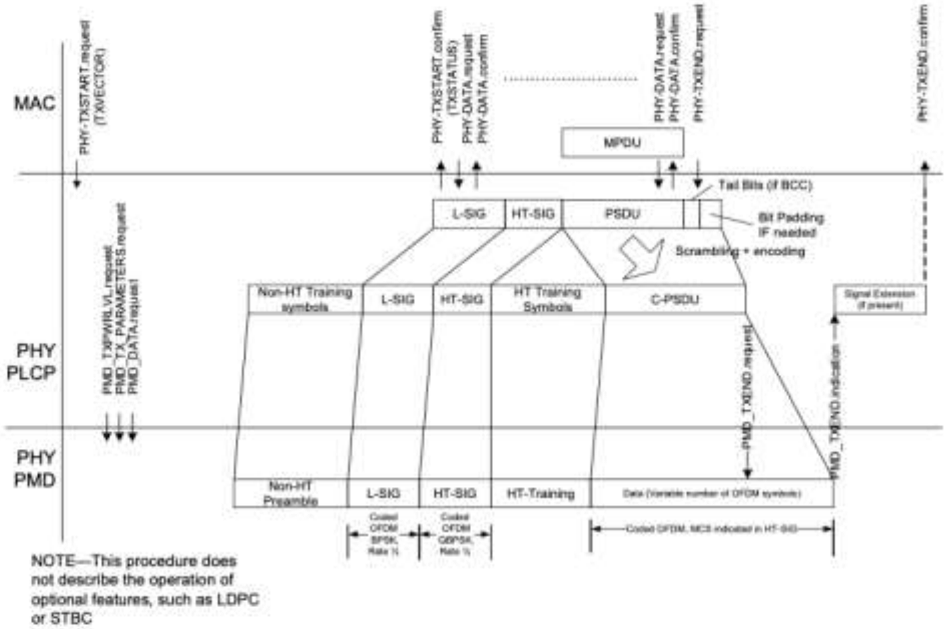
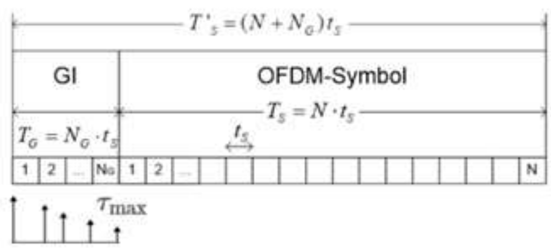


Figure 20-22—PLCP transmit procedure (HT-mixed format PPDU)

Source: IEEE Std 802.11-2012



Guard time and channel's maximum delay spread.

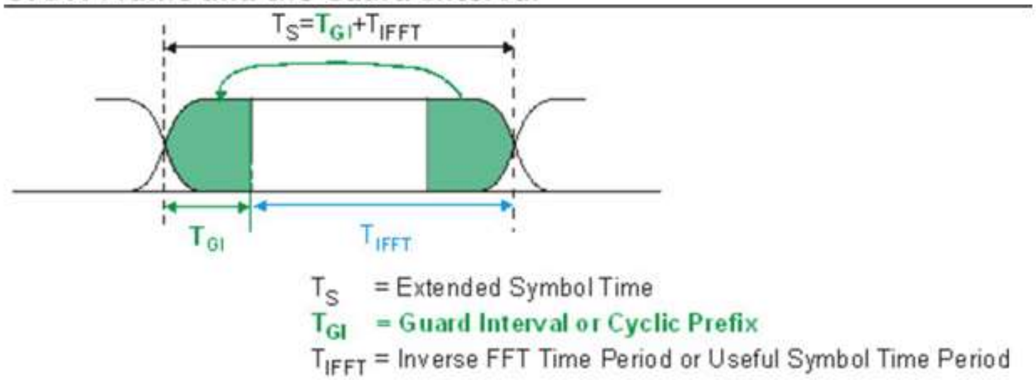
START

In this example the guard time is $T_G = 0.8\mu s$. Further settings from IEEE 802.11ac are used.

Number of subcarriers, FFT size	$N = 64$
Discrete length of the guard interval	$N_G = 16$
Data subcarriers	$N_C = 52$
Pilot subcarriers	$N_P = 4$
Extended OFDM symbol period	$T'_S = 4\mu s$
Guard interval duration	$T_G = \frac{N_G T'_s}{N+N_G} = 0.8\mu s$

Source: https://www.etti.unibw.de/labalive/experiment/ofdmguardinterval/

OFDM Frame and the Guard Interval



Typical OFDM Frame with cyclic extension

Source: https://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/Subsystems/wlan-ofdm/content/dlg_ofdm_fmt_guardintrvlfrac.htm

64. The method practiced by the '439 Accused Products includes cyclically advancing the first OFDM packet by shifting the samples in a first direction an amount less than a sample duration of the guard interval portion to generate a shifted version of the first OFDM packet for transmission.

Details and specifications for the Aruba 370 Series APs

Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance

Source: https://www.arubanetworks.com/products/wireless/access-points/outdoor-ruggedized-access-points/370-series/

20.3.3 Transmitter block diagram

HT-mixed format and HT-greenfield format transmissions can be generated using a transmitter consisting of the following blocks:

a) *Scrambler* scrambles the data to reduce the probability of long sequences of 0s or 1s; see 20.3.11.3.

i) *Inverse discrete Fourier transform (IDFT)* converts a block of constellation points to a time domain block.

j) *Cyclic shift (CSD) insertion* is where the insertion of the cyclic shifts prevents unintentional beamforming. CSD insertion may occur before or after the IDFT. There are three cyclic shift types as follows:

1) A cyclic shift specified per transmitter chain with the values defined in Table 20-9 (a possible implementation is shown in Figure 20-2).

2) A cyclic shift specified per space-time stream with the values defined in Table 20-10 (a possible implementation is shown in Figure 20-3).

3) A cyclic shift $M_{CSD}(k)$ that may be applied as a part of the spatial mapper; see 20.3.11.11.2.

k) *GI insertion* prepends to the symbol a circular extension of itself.

Source: 802.11-2012

Figure 20-2 and Figure 20-3 show example transmitter block diagrams. In particular, Figure 20-2 shows the transmitter blocks used to generate the HT-SIG of the HT-mixed format PPDU. These transmitter blocks are

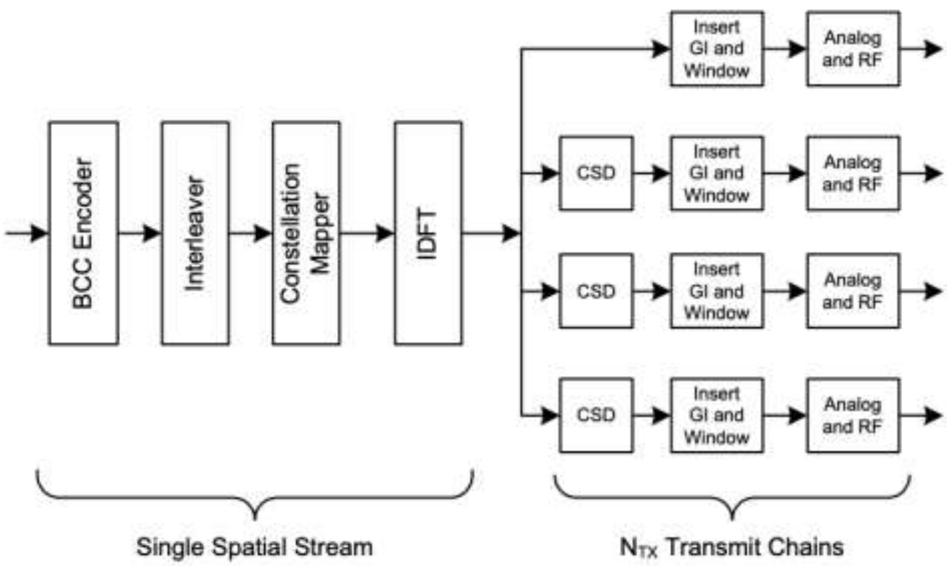


Figure 20-2—Transmitter block diagram 1

Source: 802.11-2012

20.3.9.4.3 HT-SIG definition

The HT-SIG is used to carry information required to interpret the HT packet formats. The fields of the

of 48 complex numbers: $d_{k,n}$, $0 \le k \le 47$, $n = 0, 1$. The time domain waveform for the HT-SIG in an HT-mixed format packet in a 20 MHz transmission shall be as shown in Equation (20-16).

$$r_{HT-SIG}^{i_{TX}}(t) = \frac{1}{\sqrt{N_{TX} \cdot N_{HT-SIG}^{Tone}}} \sum_{n=0}^{1} w_{T_{SYM}}(t - nT_{SYM}) \cdot \sum_{k=-26}^{26} (jD_{k,n} + p_{n+1}P_k)\exp(j2\pi k\Delta_F(t - nT_{SYM} - T_{GI} - T_{CS}^{i_{TX}})) \qquad (20\text{-}16)$$

where

$$D_{k,n} = \begin{cases} 0, k = 0, \pm 7, \pm 21 \\ d_{M'(k),n}, \text{ otherwise} \end{cases}$$

$M'(k)$ is defined in 20.3.9.3

P_k and p_n are defined in 18.3.5.10

N_{HT-SIG}^{Tone} has the value given in Table 20-8

$T_{CS}^{i_{TX}}$ represents the cyclic shift for transmit chain i_{TX} and is defined by Table 20-9 for HT-mixed format PPDUs.

Source: 802.11-2012

Table 20-6—Timing-related constants

Parameter	TXVECTOR CH_BANDWIDTH			
	NON_HT_CBW20	HT_CBW_20	HT_CBW40 or NON_HT_CBW40	
			HT format	MCS 32 and non-HT duplicate
N_{SD}: Number of complex data numbers	48	52	108	48
N_{SP}: Number of pilot values	4	4	6	4
N_{ST}: Total number of subcarriers See NOTE 1	52	56	114	104
N_{SR}: Highest data subcarrier index	26	28	58	58
Δ_F: Subcarrier frequency spacing	312.5kHz (20 MHz/64)	312.5kHz	312.5kHz (40 MHz/128)	
T_{DFT}: IDFT/DFT period	3.2 µs	3.2 µs	3.2 µs	
T_{GI}: Guard interval duration	0.8 µs= T_{DFT}/4	0.8 µs	0.8 µs	

Source: 802.11-2012

20.3.9.3.2 Cyclic shift definition

The cyclic shift values defined in this subclause apply to the non-HT fields in the HT-mixed format preamble and the HT-SIG in the HT-mixed format preamble.

Table 20-9—Cyclic shift for non-HT portion of packet

$T_{CS}^{i_{TX}}$ values for non-HT portion of packet				
Number of transmit chains	Cyclic shift for transmit chain 1 (ns)	Cyclic shift for transmit chain 2 (ns)	Cyclic shift for transmit chain 3 (ns)	Cyclic shift for transmit chain 4 (ns)
1	0	—	—	—
2	0	–200	—	—
3	0	–100	–200	—
4	0	–50	–100	–150

Source: 802.11-2012

65. The method practiced by the ’439 Accused Products includes the feature in which samples from the symbol data portion of the first OFDM packet are shifted into the guard interval portion of the shifted version and the same number of samples from the guard interval portion of the first OFDM packet are shifted out of the guard interval portion of the shifted version.

20.3.9.3.2 Cyclic shift definition

The cyclic shift values defined in this subclause apply to the non-HT fields in the HT-mixed format preamble and the HT-SIG in the HT-mixed format preamble.

Cyclic shifts are used to prevent unintentional beamforming when the same signal or scalar multiples of one signal are transmitted through different spatial streams or transmit chains. A cyclic shift of duration T_{CS} on a signal $s(t)$ on interval $0 \le t \le T$ is defined as follows, where T is defined as T_{DFT} as referenced in Table 20-6.

With $T_{CS} \le 0$, replace $s(t)$ with $s(t-T_{CS})$ when $0 \le t < T+T_{CS}$ and with $s(t-T_{CS}-T)$ when $T+T_{CS} \le t \le T$. The cyclic-shifted signal is defined as shown in Equation (20-7).

$$s_{CS}(t;T_{CS})\big|_{T_{CS}<0} = \begin{cases} s(t-T_{CS}) & 0 \le t < T+T_{CS} \\ s(t-T_{CS}-T) & T+T_{CS} \le t \le T \end{cases} \quad (20\text{-}7)$$

The cyclic shift is applied to each OFDM symbol in the packet separately. Table 20-9 specifies the values for the cyclic shifts that are applied in the L-STF (in an HT-mixed format packet), the L-LTF, and L-SIG It also applies to the HT-SIG in an HT-mixed format packet.

Source: 802.11-2012

Table 20-9—Cyclic shift for non-HT portion of packet

$T_{CS}^{i_{TX}}$ values for non-HT portion of packet				
Number of transmit chains	**Cyclic shift for transmit chain 1 (ns)**	**Cyclic shift for transmit chain 2 (ns)**	**Cyclic shift for transmit chain 3 (ns)**	**Cyclic shift for transmit chain 4 (ns)**
1	0	—	—	—
2	0	–200	—	—
3	0	–100	–200	—
4	0	–50	–100	–150

Source: 802.11-2012

Table 20-5—Timing-related constants *(continued)*

T_{DFT}: IDFT/DFT period	3.2 μs
T_{GI}: Guard interval duration	0.8 μs= $T_{DFT}/4$

Source: 802.11-2012

66. The method practiced by the ’439 Accused Products includes substantially simultaneously transmitting the first OFDM packet and the shifted version of the OFDM packet.

Figure 20-2 and Figure 20-3 show example transmitter block diagrams. In particular, Figure 20-2 shows the transmitter blocks used to generate the HT-SIG of the HT-mixed format PPDU. These transmitter blocks are

Source: 802.11-2012

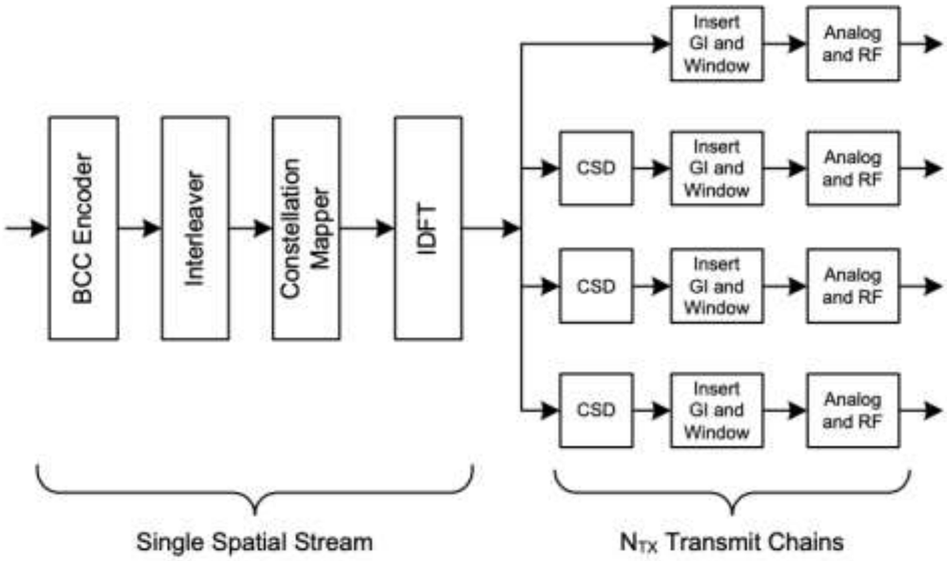


Figure 20-2—Transmitter block diagram 1

Source: 802.11-2012

b) Construct the PLCP preamble SIGNAL fields from the appropriate fields of the TXVECTOR by adding tail bits, applying convolutional coding, formatting into one or more OFDM symbols, applying cyclic shifts, applying spatial processing, calculating an inverse Fourier transform for each OFDM symbol and transmit chain, and prepending a cyclic prefix or GI to each OFDM symbol in each transmit chain. The number and placement of the PLCP preamble SIGNAL fields depend on the frame format being used. Refer to 20.3.9.3.5, 20.3.9.4.3, and 20.3.9.5.4.

c) Concatenate the PLCP preamble training and SIGNAL fields for each transmit chain one field after another, in the appropriate order, as described in 20.3.2 and 20.3.7.

r) For each group of N_{ST} subcarriers and each of the N_{TX} transmit chains, convert the subcarriers to time domain using IDFT. Prepend to the Fourier-transformed waveform a circular extension of itself, thus forming a GI, and truncate the resulting periodic waveform to a single OFDM symbol length by applying time domain windowing. Determine the length of the GI according to the GI_TYPE parameter of the TXVECTOR. Refer to 20.3.11.11 and 20.3.11.12 for details. When beamforming is not used, it is sometimes possible to implement the cyclic shifts in the time domain.

s) Append the OFDM symbols associated with each transmit chain one after another, starting after the final field of the PLCP preamble. Refer to 20.3.2 and 20.3.7 for details.

t) Up-convert the resulting complex baseband waveform associated with each transmit chain to an RF signal according to the center frequency of the desired channel and transmit. Refer to 20.3.7 for details. The transmit chains are connected to antenna elements according to ANTENNA_SET of the TXVECTOR if ASEL is applied.

Source: 802.11-2012

67. HPE has had knowledge of the ’439 patent since at least as early as the receipt of IV’s October 12, 2022 notice letter, which attached a copy of the ’439 patent, and will receive further knowledge by service upon HPE of the Complaint in this Case.

68. Additionally, HPE has been and currently is an active inducer of infringement of the ’439 patent under 35 U.S.C. § 271(b) and a contributory infringer of the ’439 patent under 35 U.S.C. § 271(c).

69. HPE has actively induced and continues to actively induce infringement of the ’439 patent by causing others to use, offer for sale, or sell products or services covered by the ’439 patent, including the ’439 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end users who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the ’439 patent. HPE’s inducement includes the directions and instructions found at:

- https://support.hpe.com/hpesc/public/docDisplay?docId=a00036501en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00062129en_us
- https://www.arubanetworks.com/techdocs/hardware/aps/ap203h/ig/203H%20IG%20Rev01_Online_EN.pdf
- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00062129en_us

70. HPE has contributed to and continues to contribute to the infringement of the ’439 patent by others by selling the ’439 Accused Products, which, when installed, configured, and used, directly infringe the ’439 patent.

71. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of the ’439 patent.

72. HPE has committed and continues to commit contributory infringement by selling products and services that directly infringe the ’439 patent when used by a third party, such as the ’439 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the ’439 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

73. As a result of HPE’s acts of infringement, Intellectual Ventures I has suffered and will continue to suffer damages in an amount to be determined at trial.

PRAYER FOR RELIEF

Plaintiffs request that the Court enter judgment:

(A) that HPE has infringed the asserted patents;

(B) awarding damages sufficient to compensate plaintiffs for HPE’s infringement under 35 U.S.C. § 284;

(C) finding this case exceptional under 35 U.S.C. § 285 and awarding plaintiffs their reasonable attorneys’ fees;

(D) awarding plaintiffs the costs and expenses incurred in this action;

(E) awarding prejudgment and post-judgment interest; and

(F) granting such further relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand trial by jury of all claims so triable under Federal Rule of Civil Procedure 38.

Dated: October 13, 2022

Respectfully submitted,

OF COUNSEL:

Matthew D. Vella
mvella@princelobel.com
Robert R. Gilman
rgilman@princelobel.com
Jonathan DeBlois
jdeblois@princelobel.com
James J. Foster
jfoster@princelobel.com
Aaron S. Jacobs
ajacobs@princelobel.com
PRINCE LOBEL TYE LLP
One International Place, suite 3700
Boston, MA 02110
Tel: 617-456-8000

FARNAN LLP

/s/ Michael J. Farnan
Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market Street, 12th floor
Wilmington, DE 19801
Tel: 302-777-0300
Fax: 302-777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com